Sri Lanka Institute of Information Technology

Individual Assignment

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19187488	Y.K.Lumindu Dilumka

Link to the video-
https://mysliit.sharepoint.com/sites/WSAssignment874/Shared%20Documents/General/Final%20Video/IT19187488.mp4

Objective

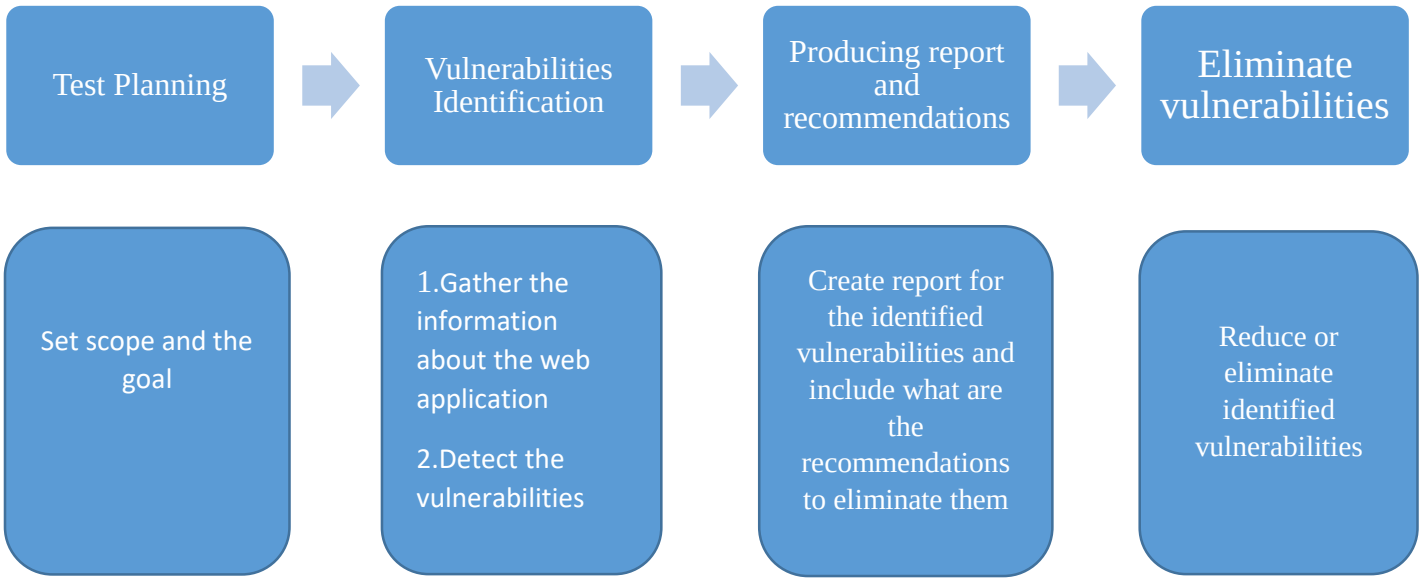
The aim of this evaluation is to define web application vulnerabilities and to show the resulting degree of risk associated with the vulnerabilities.

Application Credentials and URL

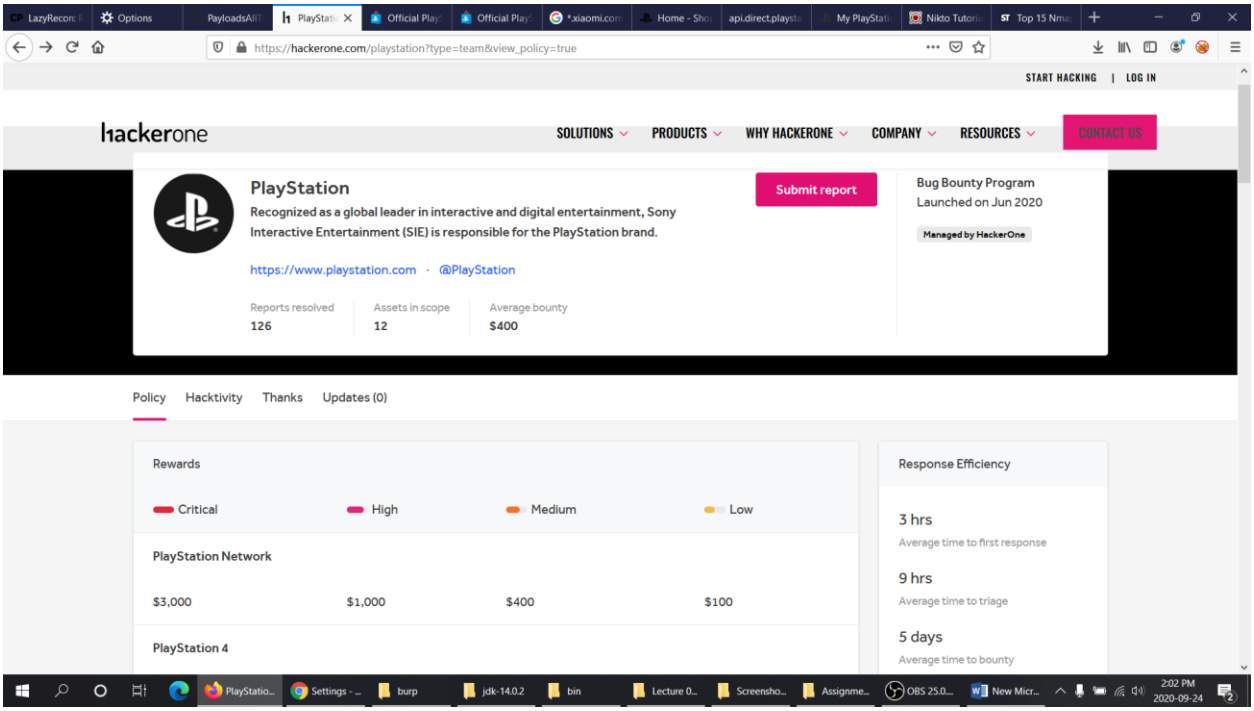
https://hackerone.com/playstation?type=team&view_policy=true

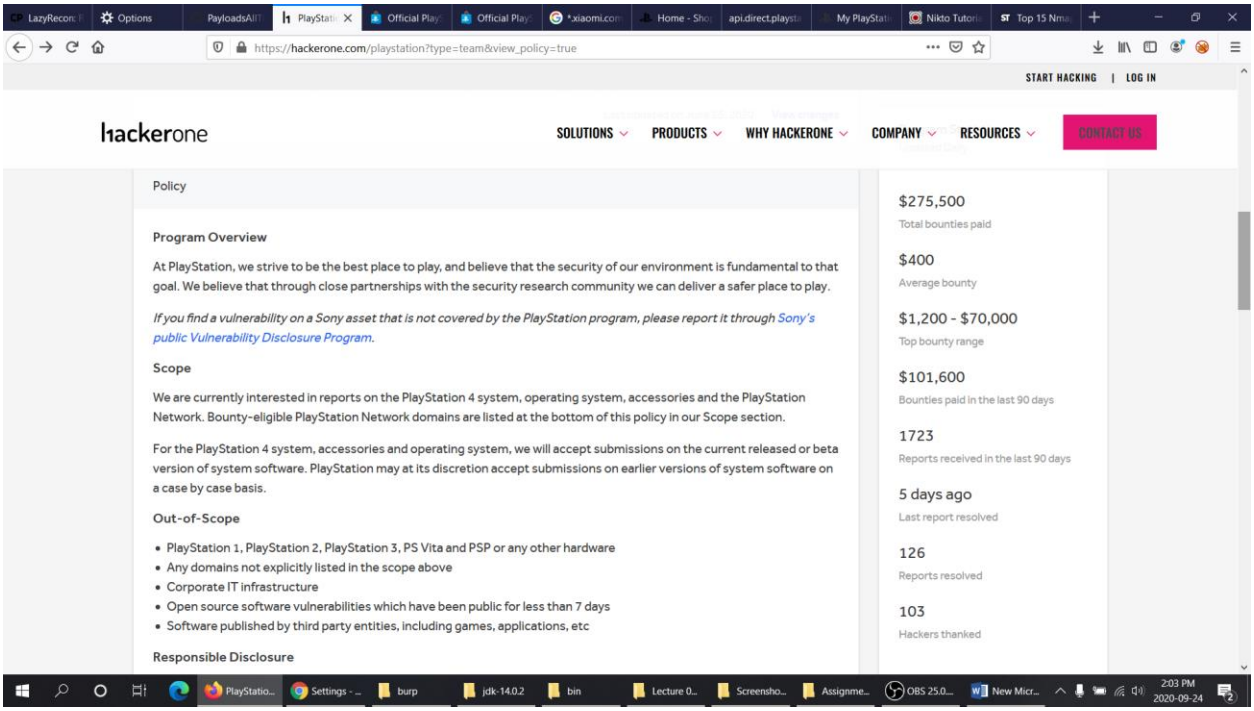
Methodology

In order to uncover the broad variety of flaws, a blended approach is adopted to conduct the evaluation that is a mixture of methods. In addition, the evaluation is adaptive in the sense of nature helps them to monitor the appraisal technique to concentrate on the sensitive areas of the program in compliance with the application features. The attack vectors are managed according to the needs of the evaluation and the selection of the attack ensures optimum application coverage.

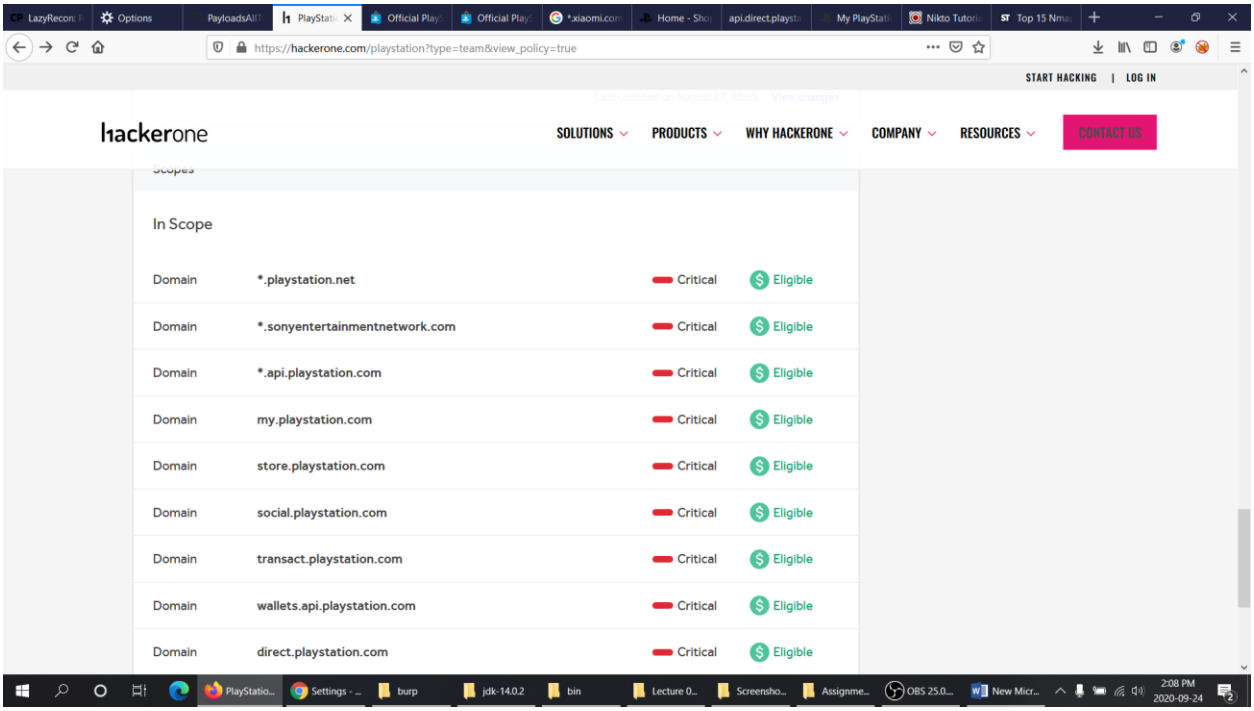


This is the website which I'm going to use for the web audit assignment.They clearly display the bounty systems which they provide for the researchers and also there are policies that we should allowed to do when we are doing the web audit.

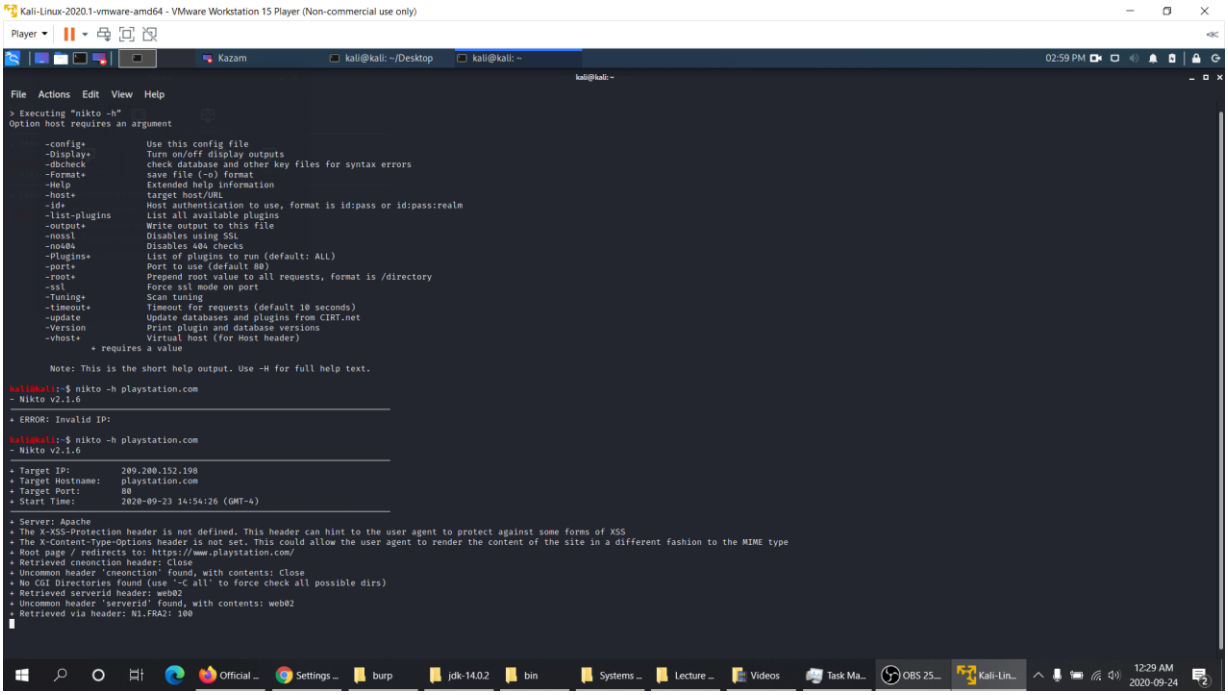




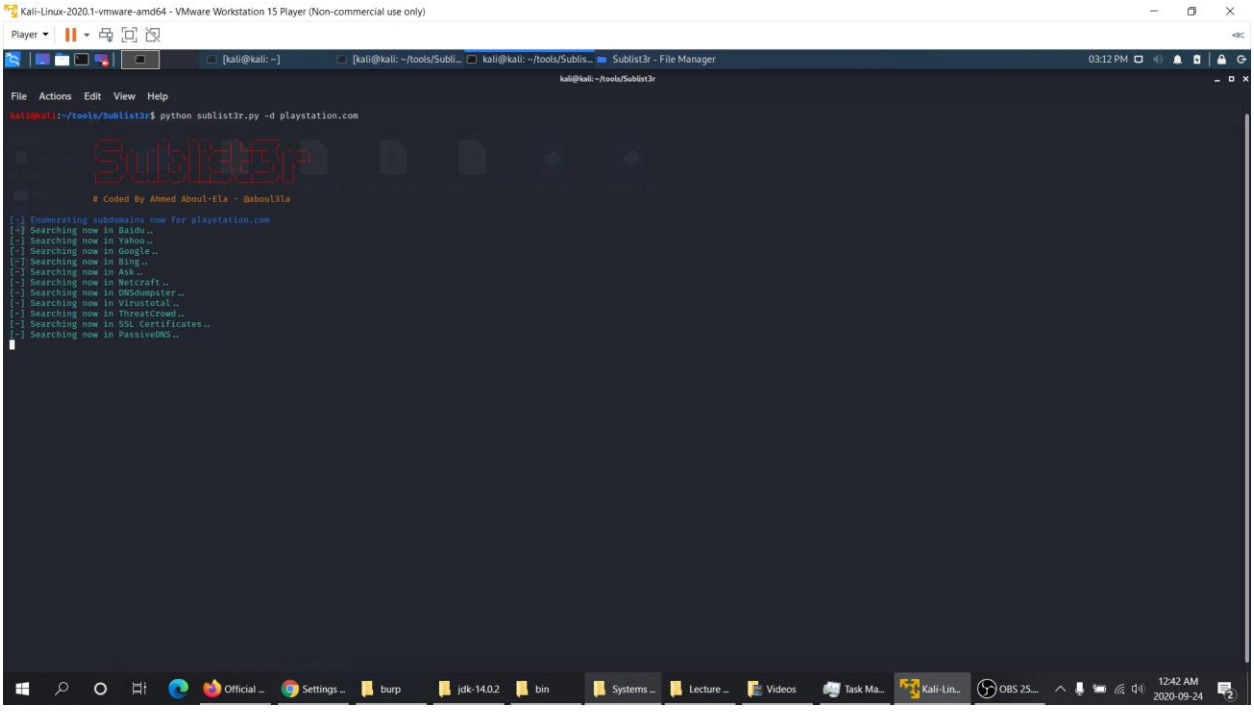
Scope



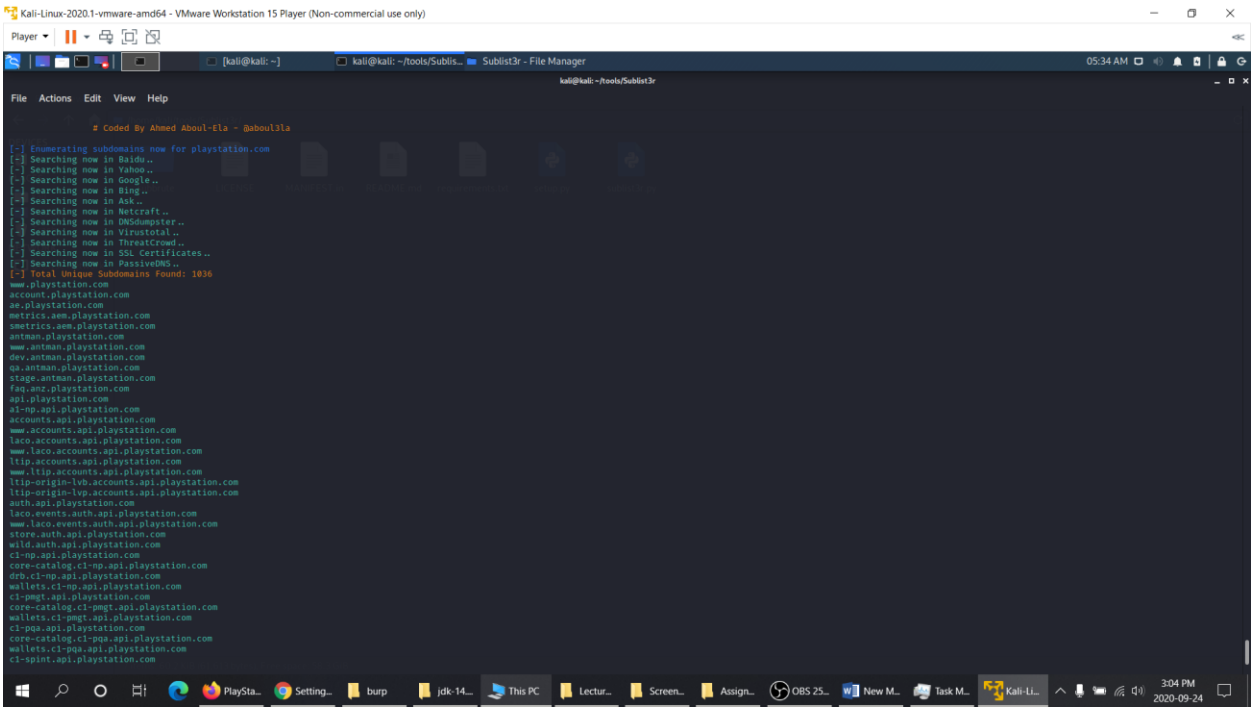
First of all im going to do some recon using linux tools to get a better understanding about the domain.The first recon tool which im going to use is nikto.It can find details about Ip,Port,the start time,server and lot of other details.



And also there's a tool called sublist3r which will search subdomains below in these search engines and details about SSL certificates to gives a better idea about the domain.

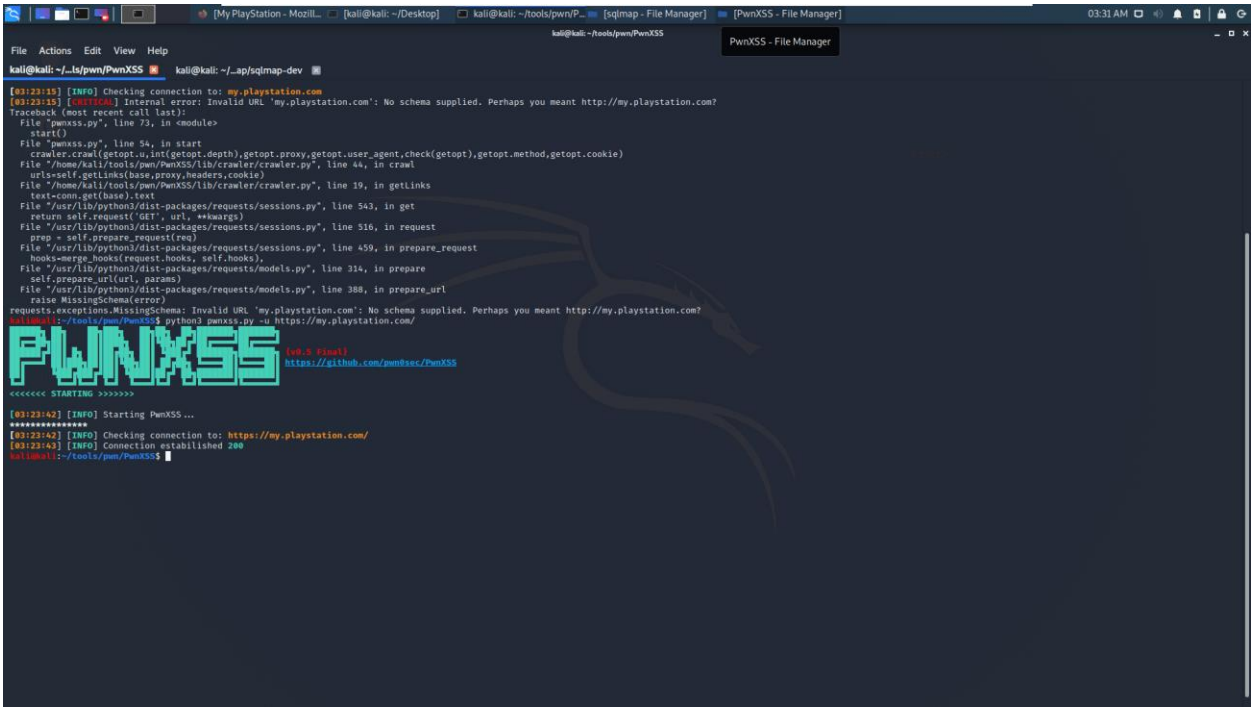


After the scan you can see more than thousands of unique subdomains are listed in playstation.com.

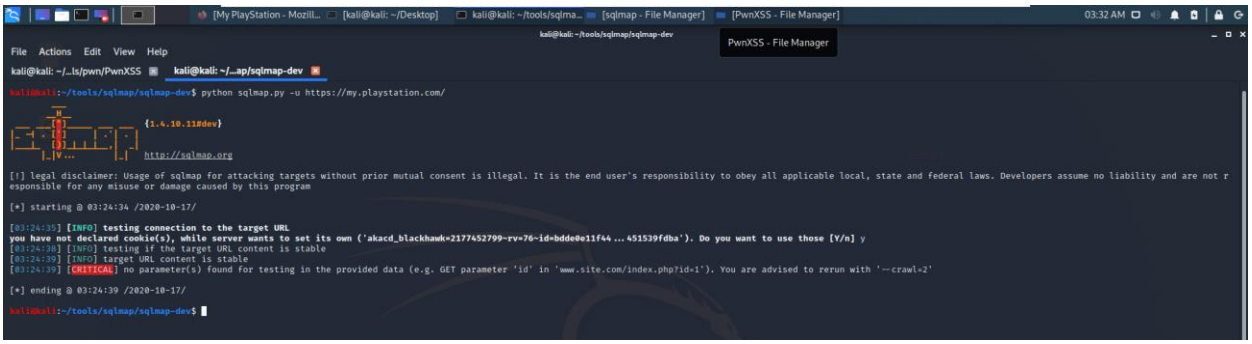


1. Im going to use **my.playstation.com** to find vulnerabilities using few tools.

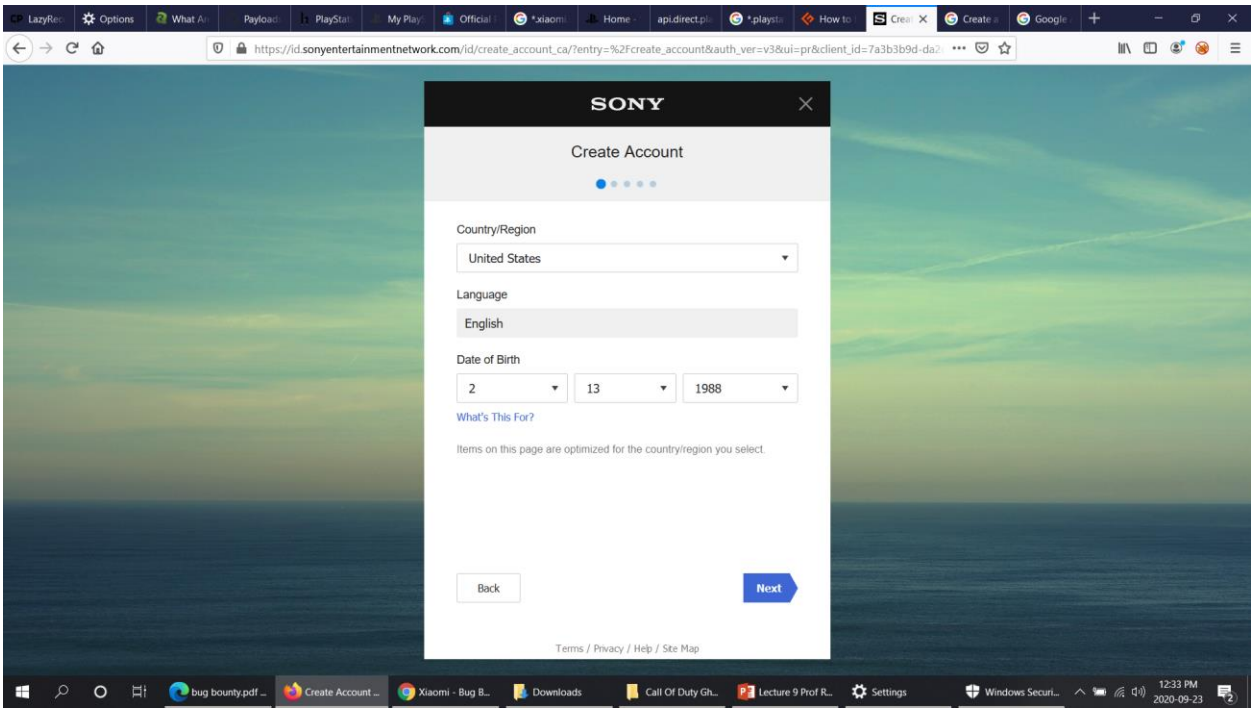
I did a pwnXSS scan to find some xss vulnerabilities. But there was no issues with xss vulnerabilities.



Then I perform a sqlmap to find whether this domain is vulnerable to sql injection flaws.After the scan I found only 1 critical vulnerability.

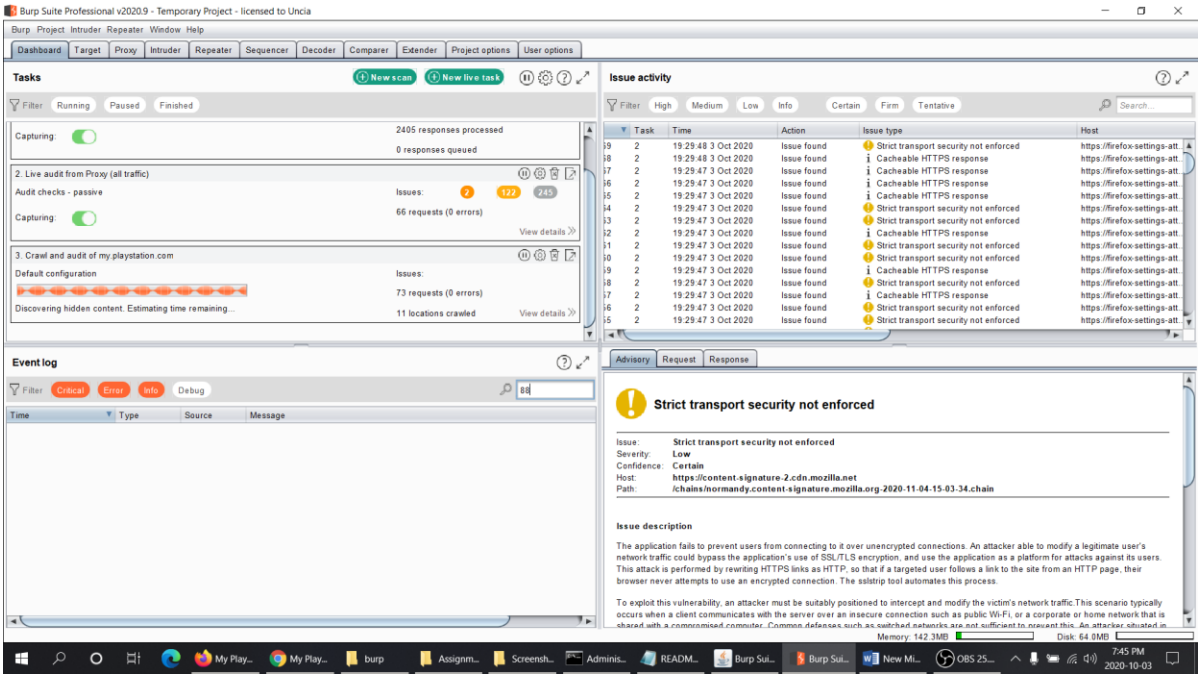


I have created an account on **my.playstation.com**

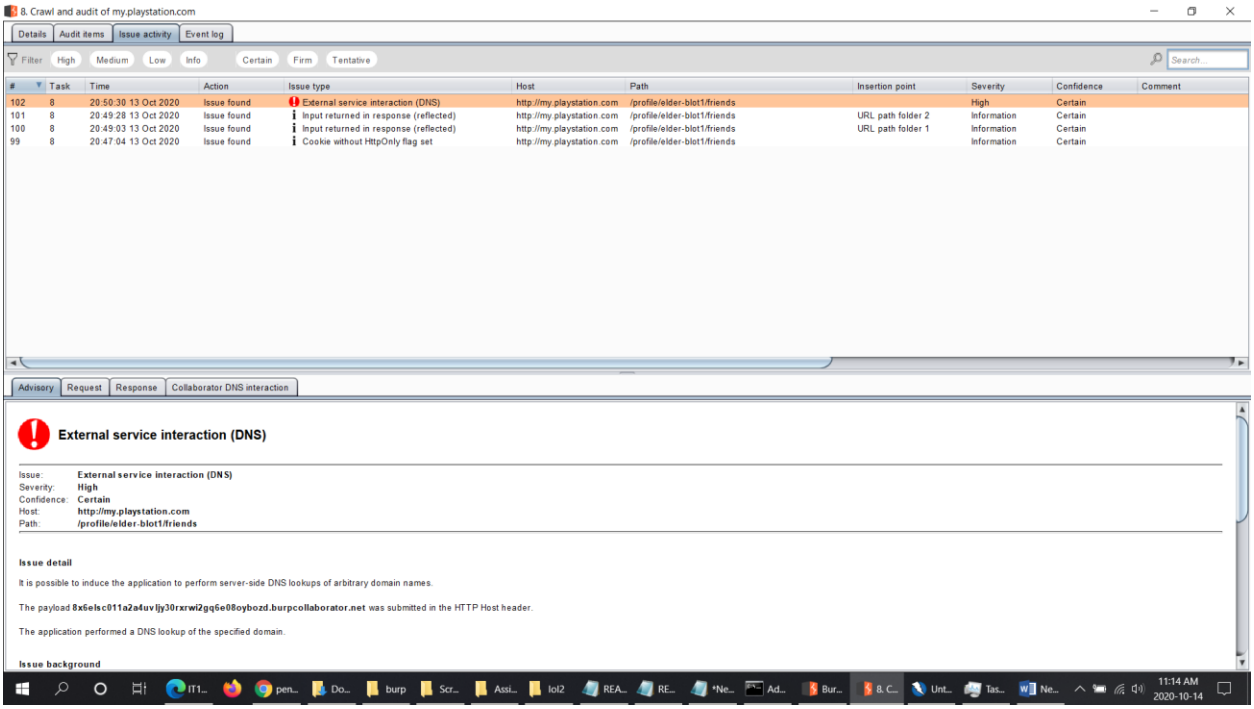


After creating the account I just figure out what are the features can do it in this domain and I click every button to get a clear idea.

I’m also going to use burp suite to scan the vulnerabilities in my.playstation.com



After the scan you will able to see some issues are found from low to high.



Server-Side Request Forgery (SSRF)

Vulnerability title:

External Service Interaction(DNS)

Risk rating:

Severity: High

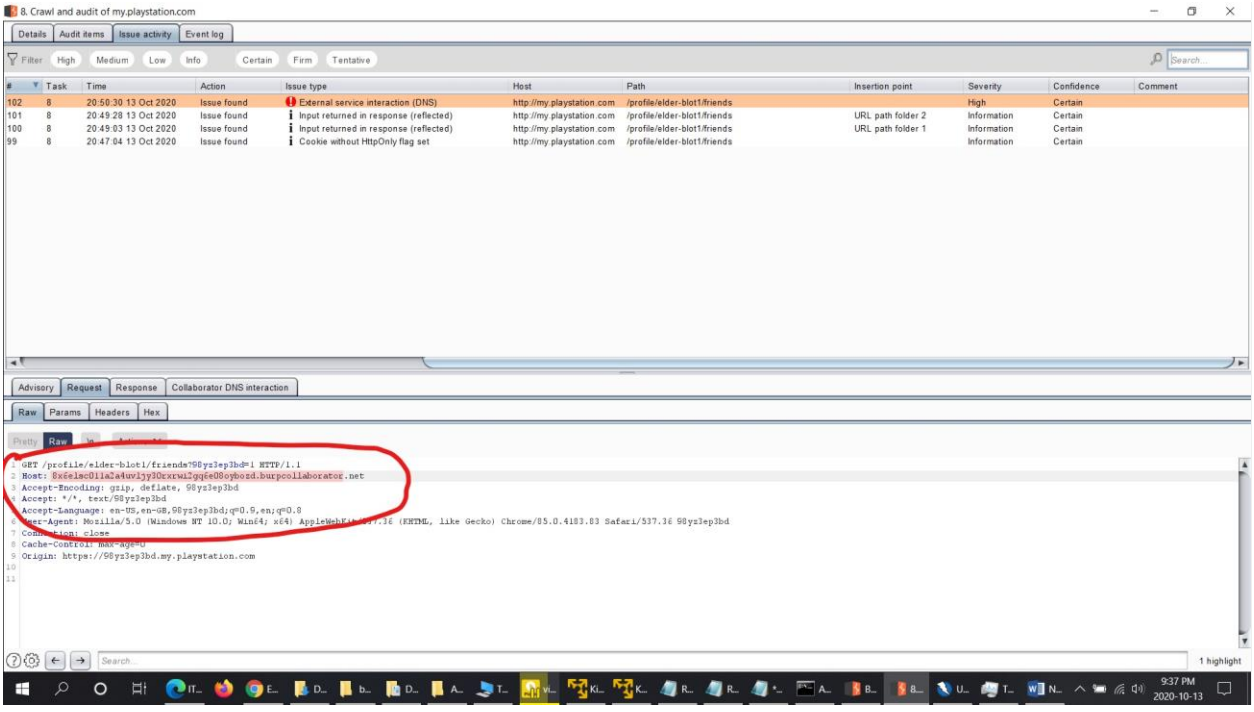
Description:

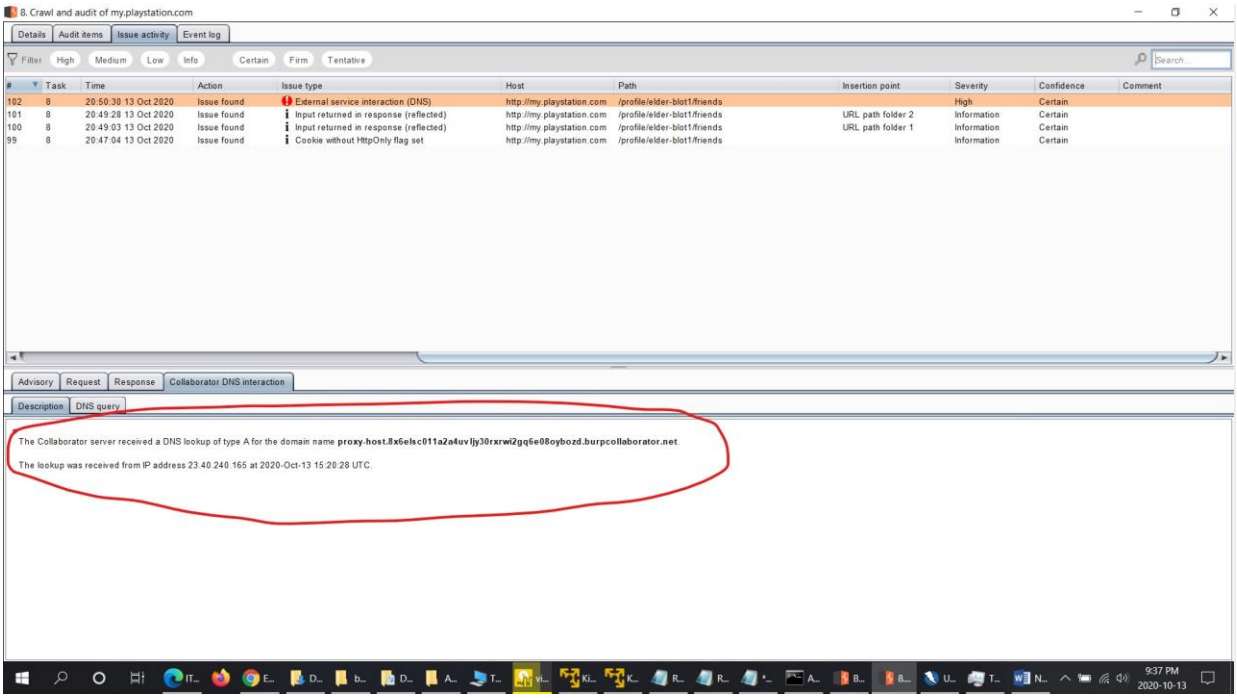
External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences. The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy.

Why: Blind Amplified DNS based DDOS

How:

If a payload starting "http://..." causes a DNS-only interaction, then this strongly indicates that outbound HTTP from the server is being blocked. In this situation, a follow-up attack could target public DNS servers. Such weakness in application could be much severe with HPP where payload pushed contains multiple “https://...” values.





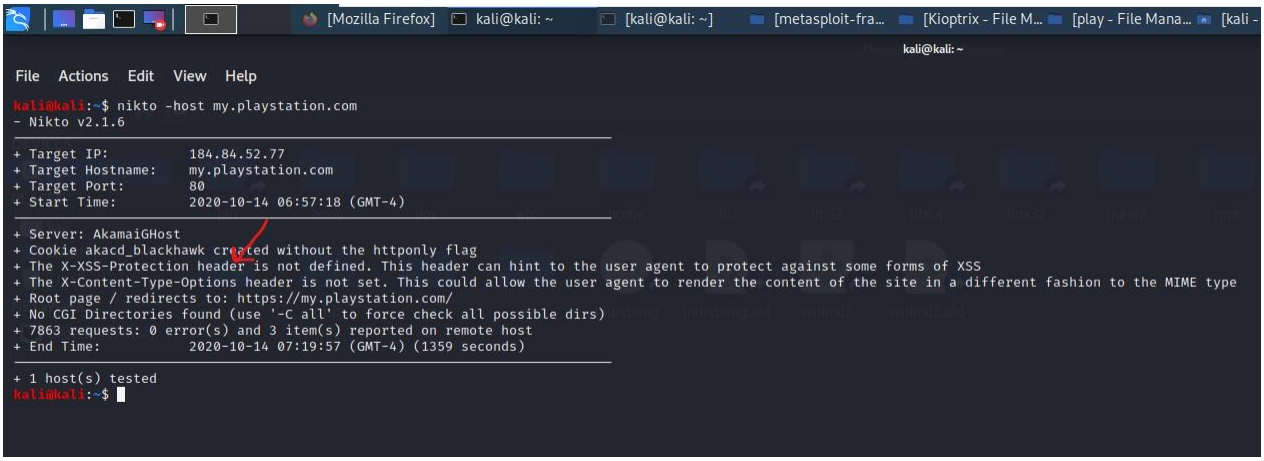
Impact:

We can use the weakness as a attack proxy to DDOS all Internal/external web conatiners, also could be amplified too.

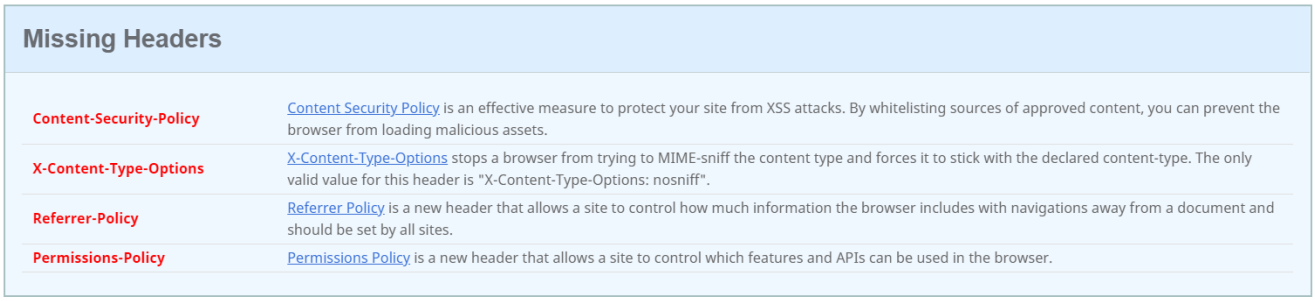
Mitigate threat:

- Review source code for functions such as dns.resolve(), dns.query() etc.
- Use whitelist check, boundary based validation and sanitization
- Maintain whitelist at network and web front

When scaning my.playstaion.com using nikto there are some issues regarding the headers.Also there have to be some missing important headers that should include.

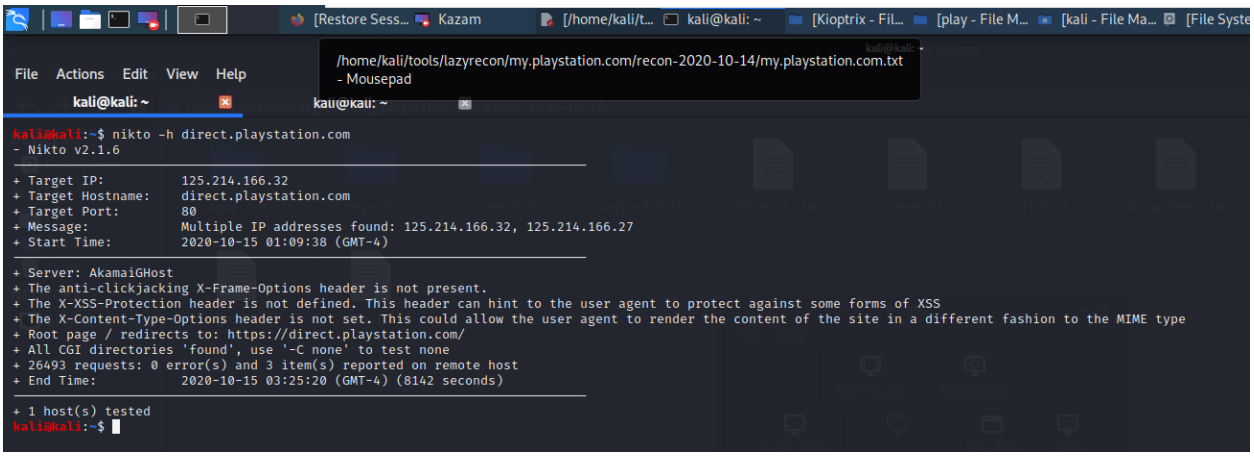


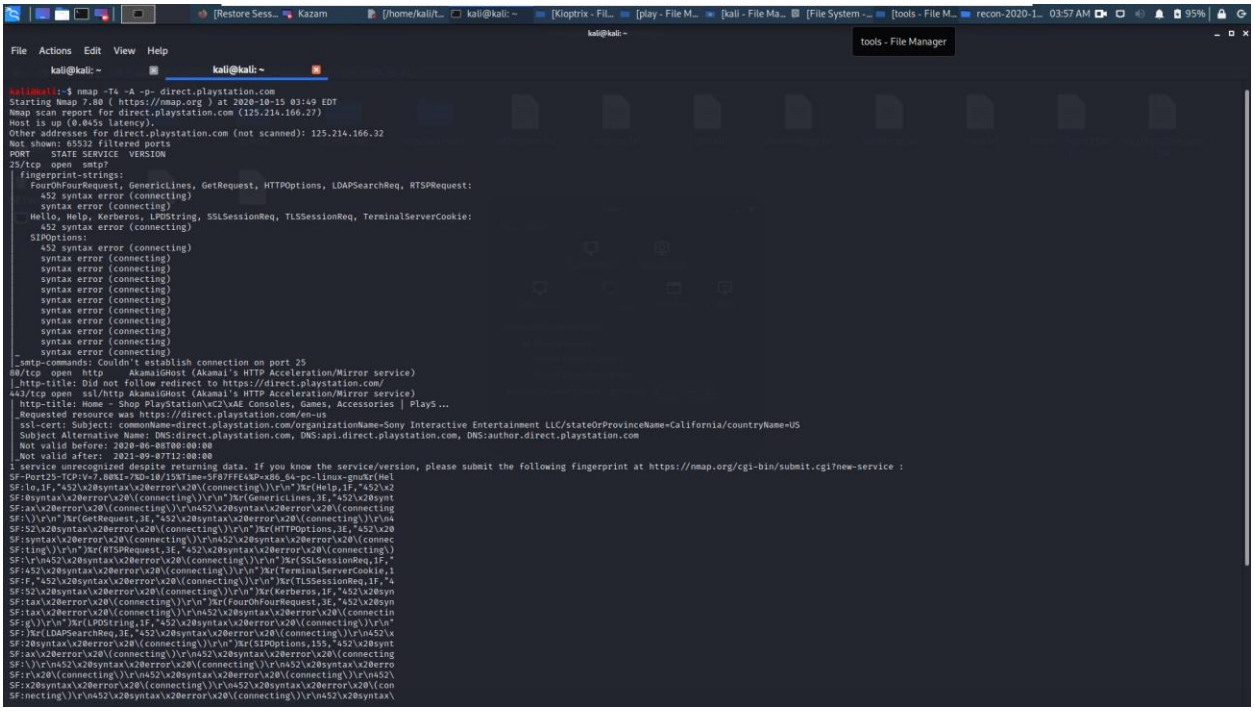
These are the missing headers that should include(Source- https://securityheaders.com/)



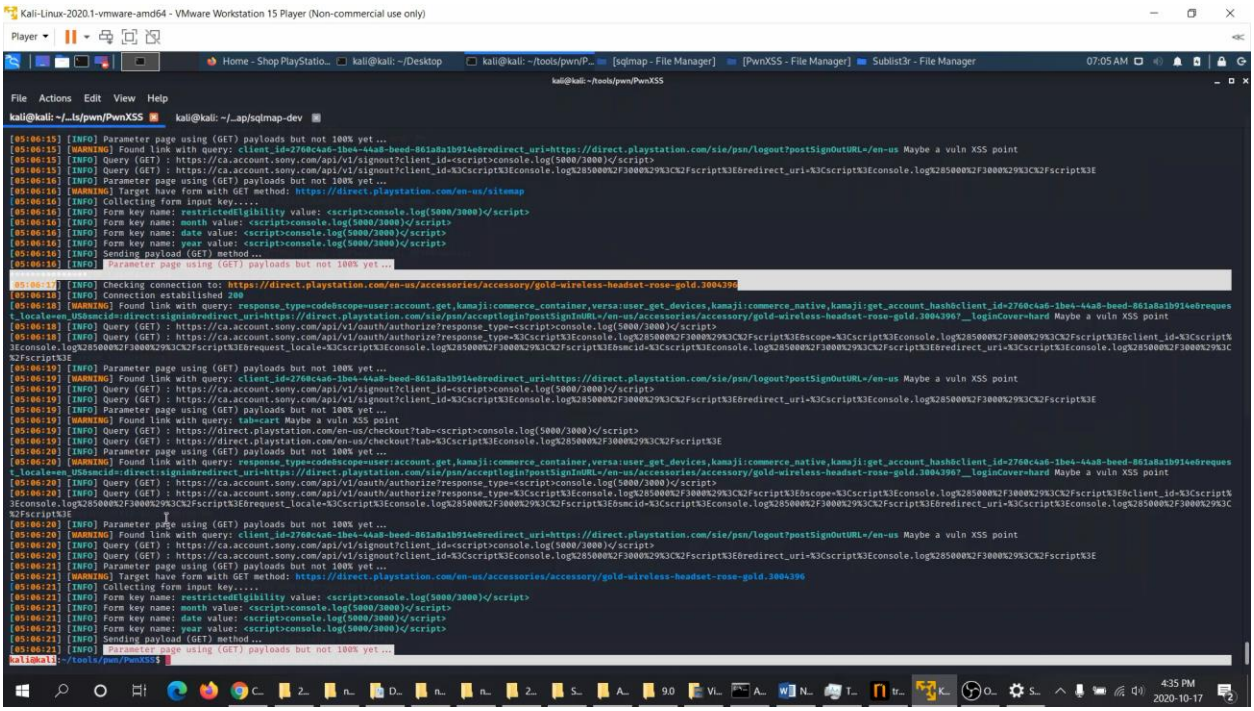
2. The second domain which I scanned is https://direct.playstation.com/en-us

Here are the results using recon tools,

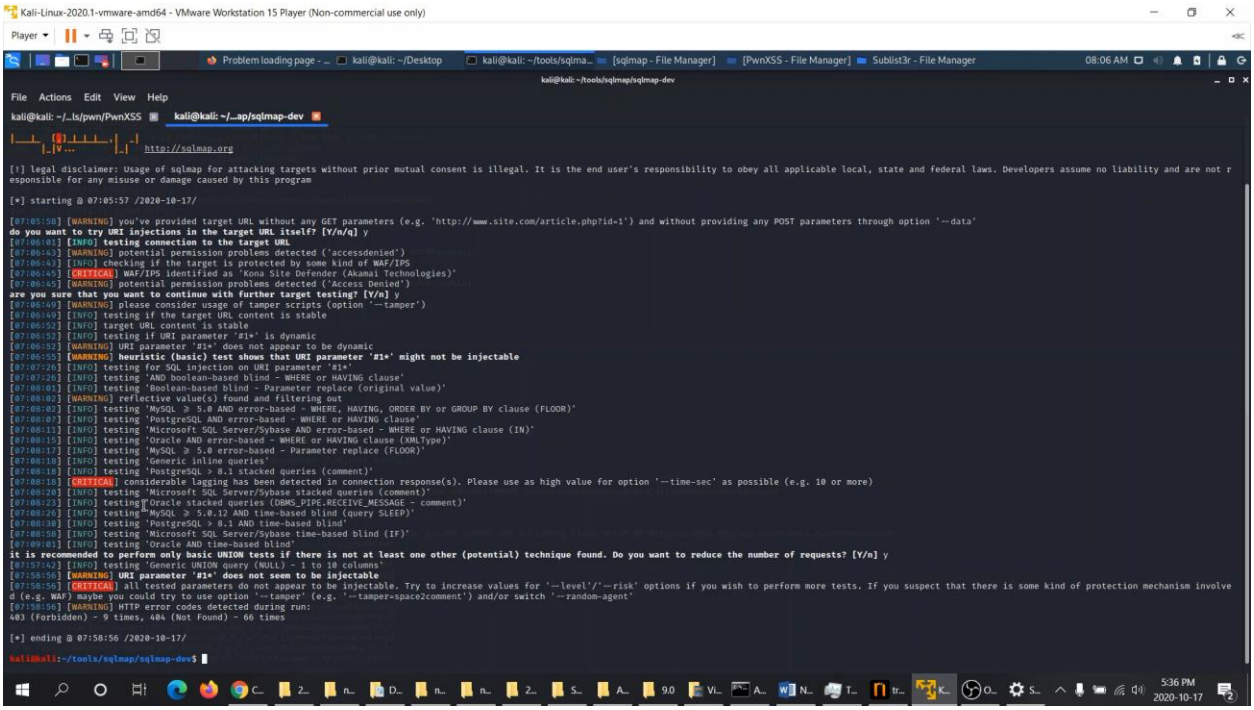




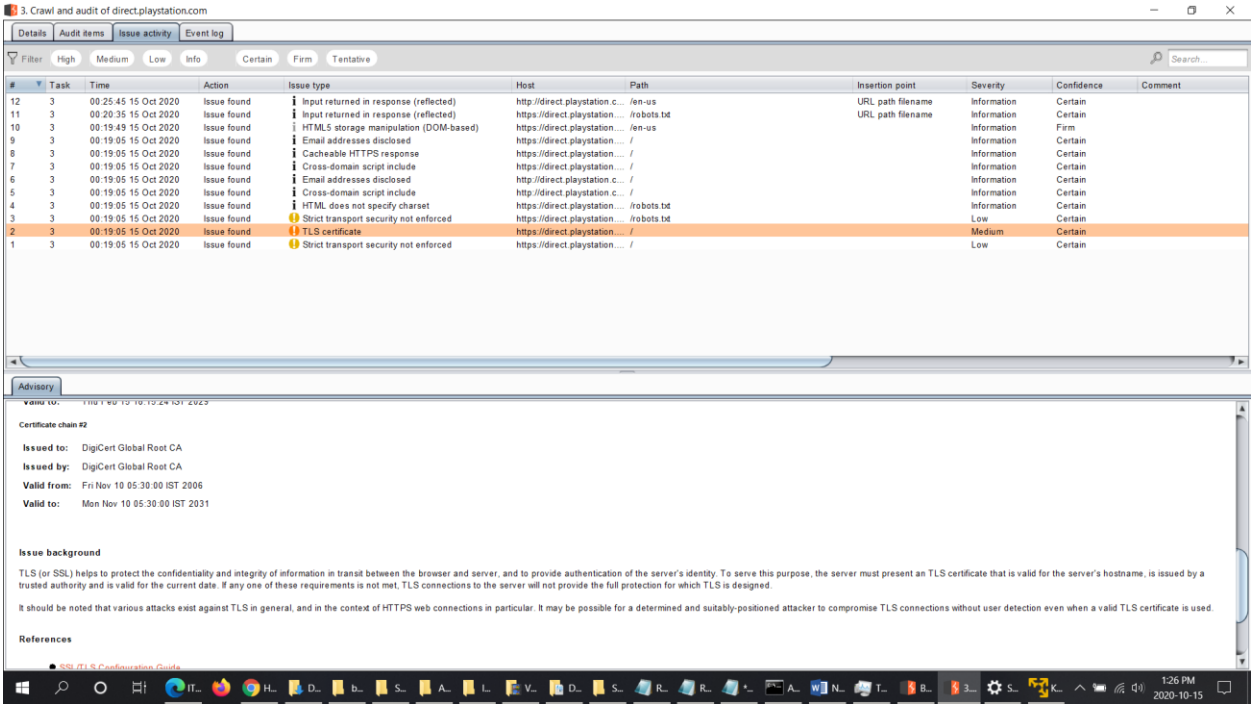
pwnXSS scan results,



Sqlmap results,



This is the result after scan through burp suite and we can see some useful vulnerabilities are shown.



Encryption and Authentication

Vulnerability title:

TLS Certificate

Risk rating:

Severity: Medium

Description:

Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve

this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

Impact:

Exploits in the wild may target flaws in the TLS protocol, including weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities or any combination of the above.

Mitigate threat:

- Establish their security baseline with a real-time, comprehensive overview of SSL certificates and their termination endpoints across the entire network.
- Detect vulnerabilities via scanning for problematic certificates or server configurations and easily review results using Certificate Inspector’s intuitive dashboard.
- Analyze security data points either by aggregate or specific to each certificate and endpoint.
- Mitigate discovered vulnerabilities, such as BEAST, and lack of compliance with industry guidelines such as the CA/Browser Forum Baseline Requirements, through recommended steps.

Vulnerability title:

Strict transport security not enforced

Risk rating:

Severity: Low

Description:

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link

to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Impact:

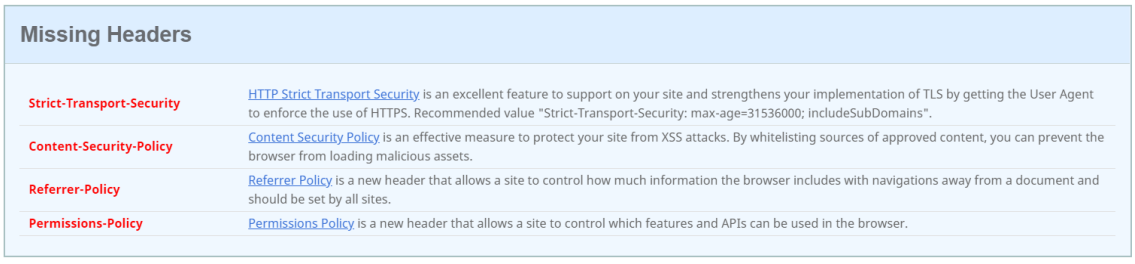
- User bookmarks or manually types http://example.com and is subject to a man-in-the-middle attacker
- HSTS automatically redirects HTTP requests to HTTPS for the target domain
- Web application that is intended to be purely HTTPS inadvertently contains HTTP links or serves content over HTTP
- A man-in-the-middle attacker attempts to intercept traffic from a victim user using an invalid certificate and hopes the user will accept the bad certificate
- HSTS does not allow a user to override the invalid certificate message

Mitigate threat:

- If the site owner would like their domain to be included in the HSTS preload list maintained by Chrome (and used by Firefox and Safari), then use the header below.
  `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`

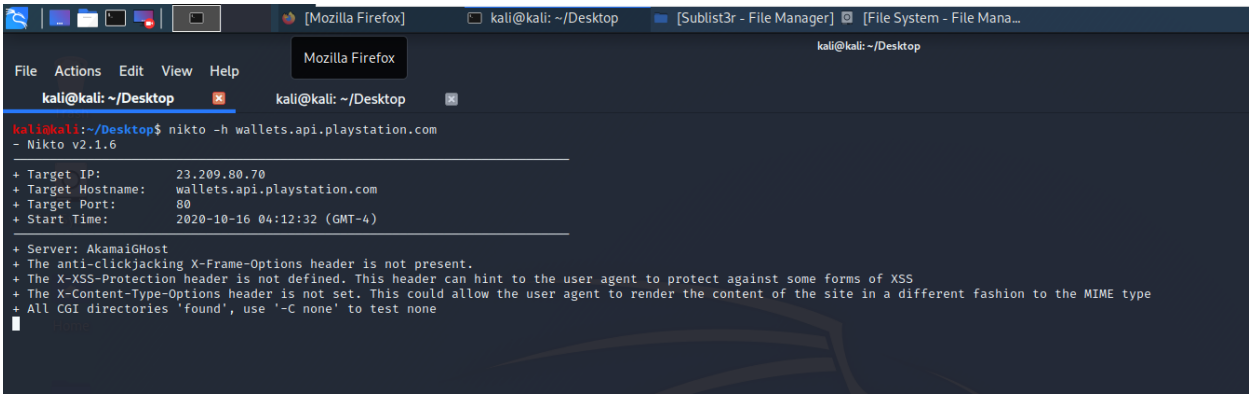
- Sending the preload directive from your site can have PERMANENT CONSEQUENCES and prevent users from accessing your site and any of its subdomains if you find you need to switch back to HTTP. Please read the details at preload removal before sending the header with preload.

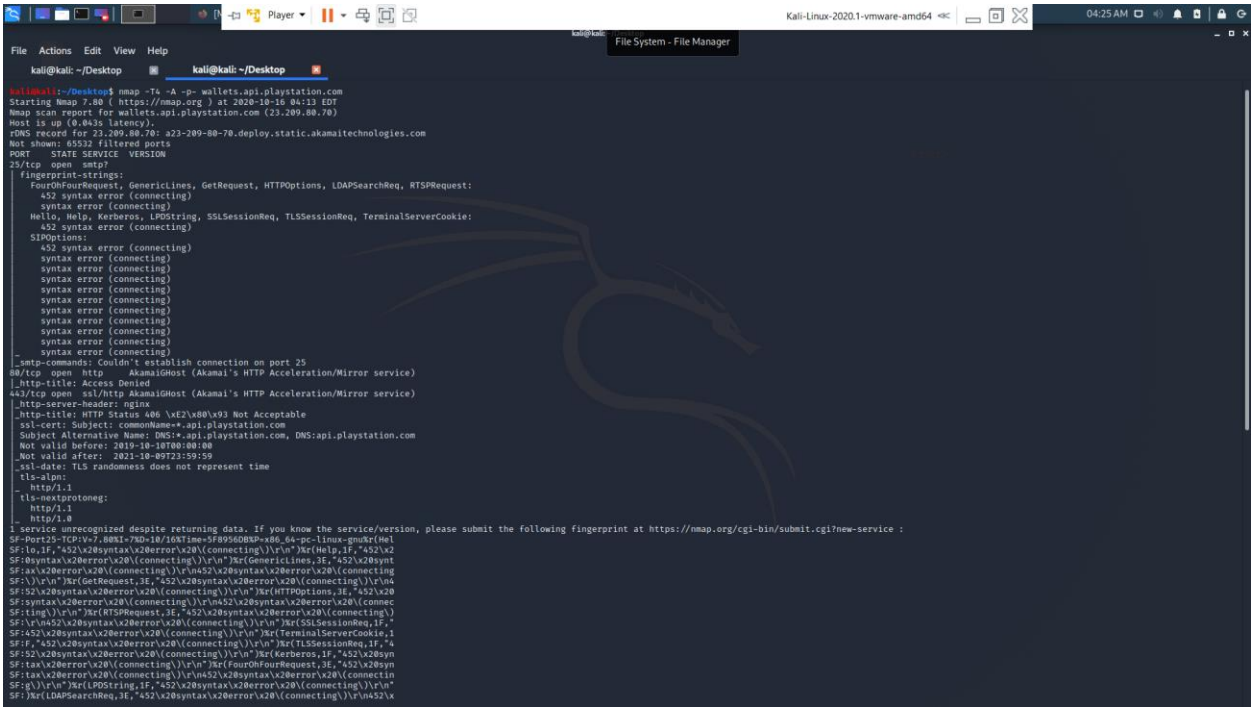
These are the missing headers that should include,

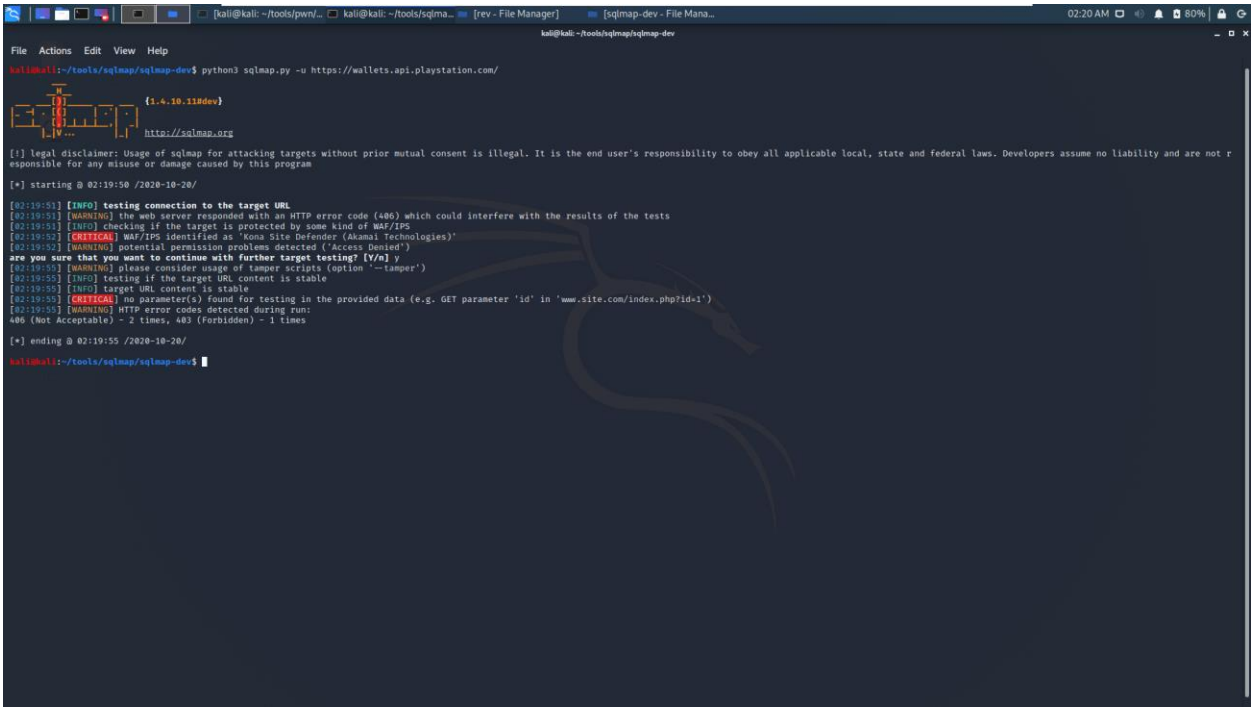


3. wallets.api.playstation.com

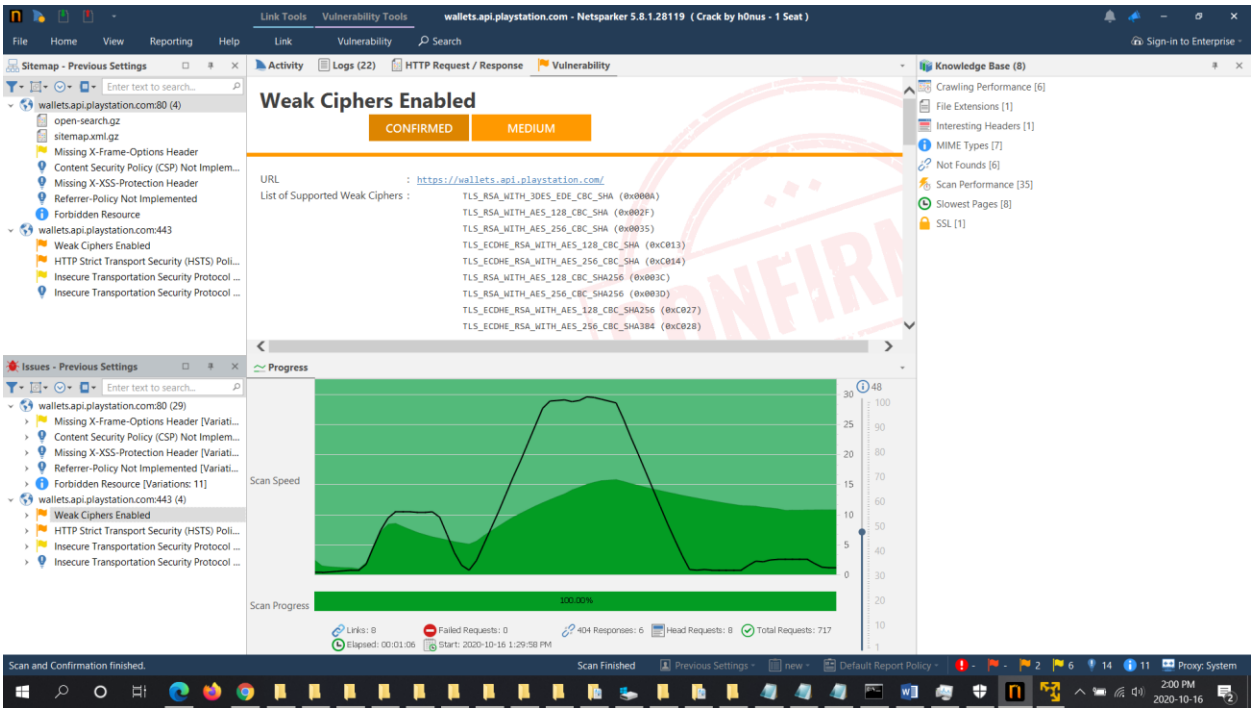
Here are the results using recon tools,







instead of using burp I used netsparker to scan remaining domains.here are the results,



Vulnerability title:

Weak Ciphers Enabled

Risk rating:

Severity: Medium

Description:

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

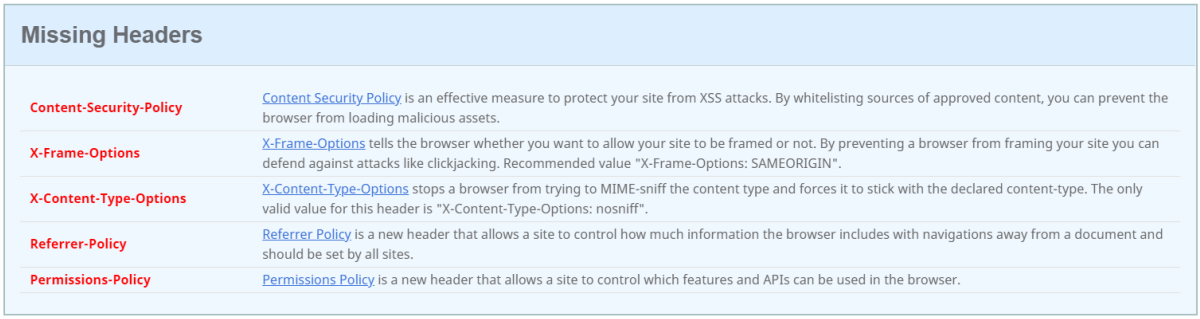
Impact:

Attackers might decrypt SSL traffic between your server and your visitors.

Mitigate threat:

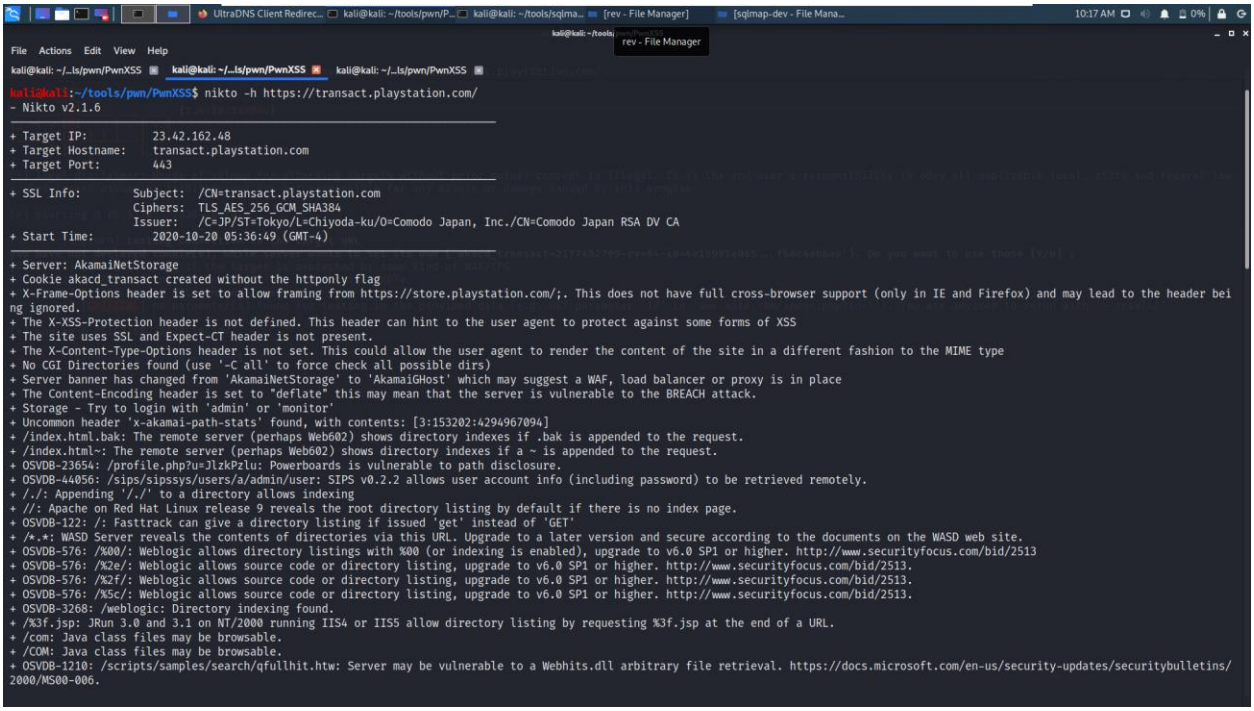
Configure your web server to disallow using weak ciphers

These are the missing headers that should include,

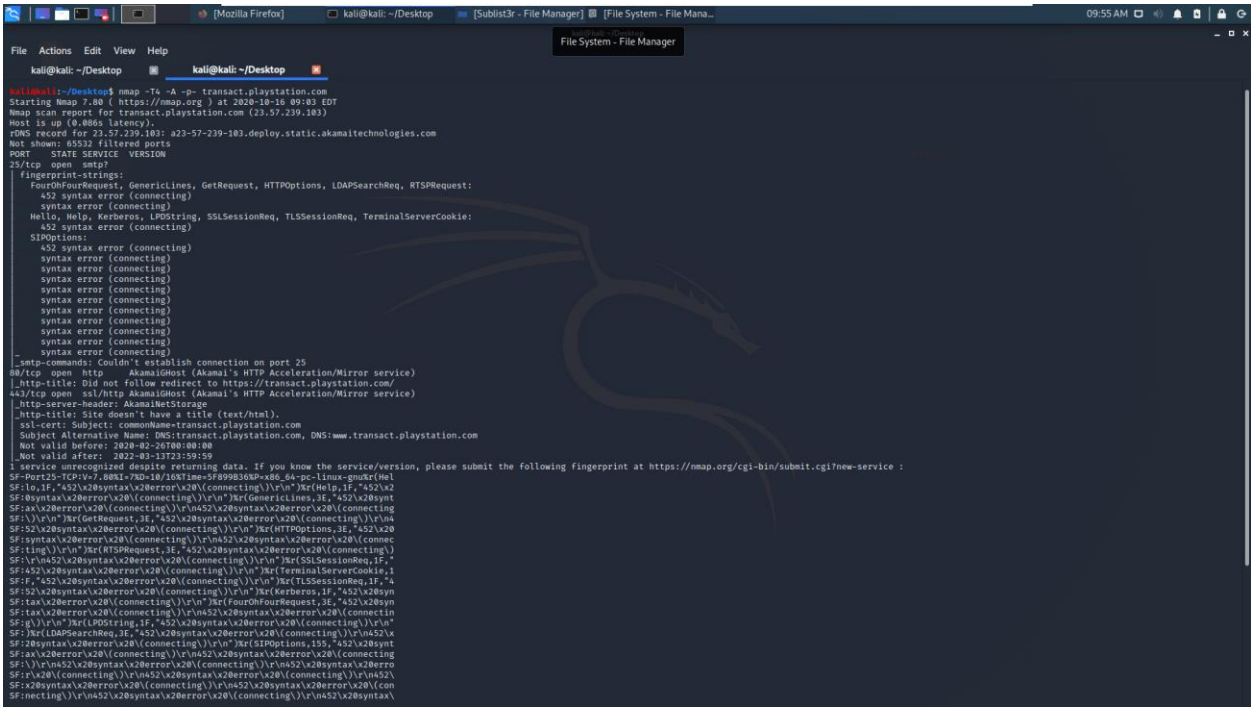


4.**transact.playstation.com**

Here are the results using recon tools,

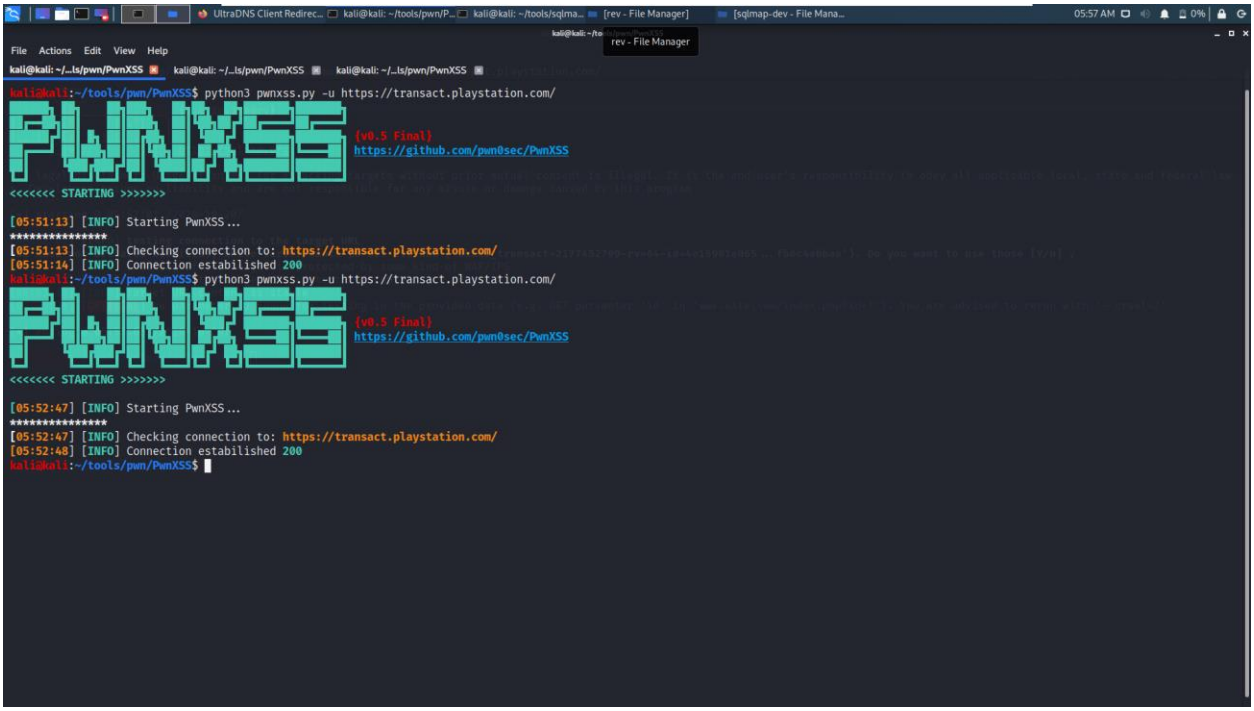


```
kali@kali:~/tools/pwn/PwnXSS$ nikto -h https://transact.playstation.com/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          23.42.162.48
+ Target Hostname:    transact.playstation.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=transact.playstation.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=JP/ST=Tokyo/L=Chiyoda-ku/O=Comodo Japan, Inc./CN=Comodo Japan RSA DV CA
+ Start Time:         2020-10-20 05:36:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiNetStorage
+ Cookie akacd_transact created without the httponly flag
+ X-Frame-Options header is set to allow framing from https://store.playstation.com/;. This does not have full cross-browser support (only in IE and Firefox) and may lead to the header bei
ng ignored.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'AkamaiNetStorage' to 'AkamaiGHost' which may suggest a WAF, load balancer or proxy is in place
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Storage - Try to login with 'admin' or 'monitor'
+ Uncommon header 'x-akamai-path-stats' found, with contents: [3:153202:4294967094]
+ /index.html.bak: The remote server (perhaps Web602) shows directory indexes if .bak is appended to the request.
+ /index.html~: The remote server (perhaps Web602) shows directory indexes if a ~ is appended to the request.
+ OSVDB-23654: /profile.php?u=JlzkPzlu: Powerboards is vulnerable to path disclosure.
+ OSVDB-44056: /sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely.
+ /./: Appending '/./' to a directory allows indexing
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-122: /: Fasttrack can give a directory listing if issued 'get' instead of 'GET'
+ /*.*: WASD Server reveals the contents of directories via this URL. Upgrade to a later version and secure according to the documents on the WASD web site.
+ OSVDB-576: /%00/: Weblogic allows directory listings with %00 (or indexing is enabled), upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-576: /%2f/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-576: /%5c/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /weblogic: Directory indexing found.
+ /%3f.jsp: JRun 3.0 and 3.1 on NT/2000 running IIS4 or IIS5 allow directory listing by requesting %3f.jsp at the end of a URL.
+ /com: Java class files may be browsable.
+ /COM: Java class files may be browsable.
+ OSVDB-1210: /scripts/samples/search/qfullhit.htw: Server may be vulnerable to a Webhits.dll arbitrary file retrieval. https://docs.microsoft.com/en-us/security-updates/securitybulletins/
2000/MS00-006.
```

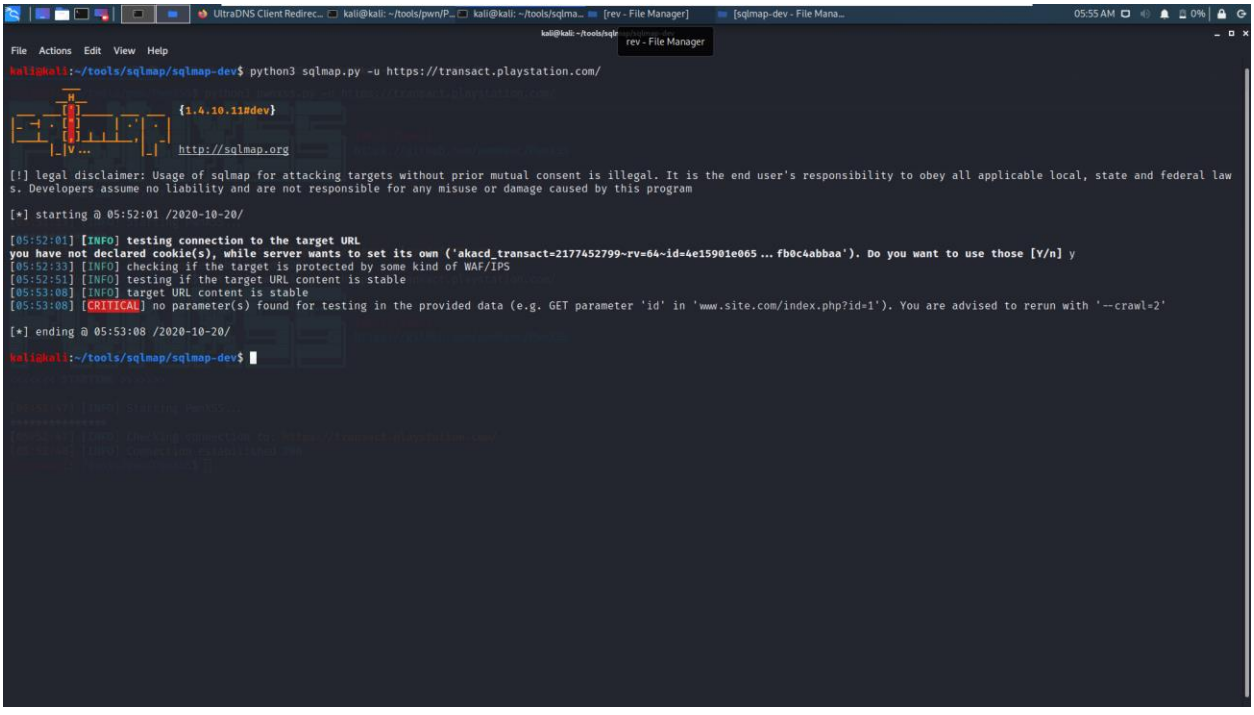


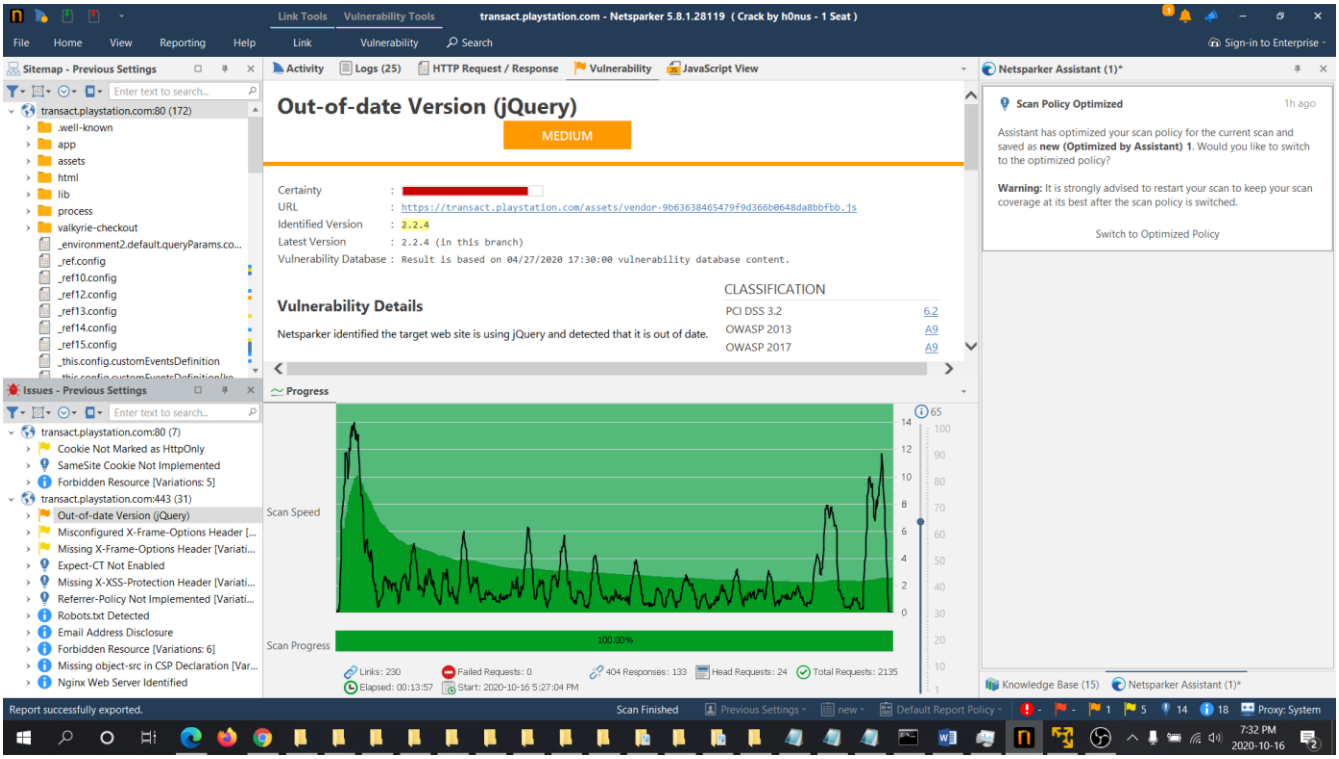
```
kali@kali:~/Desktop$ nmap -T4 -A -p- transact.playstation.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 09:03 EDT
Nmap scan report for transact.playstation.com (23.57.239.103)
Host is up (0.086s latency).
rDNS record for 23.57.239.103: a23-57-239-103.deploy.static.akamaitechnologies.com
Not shown: 65532 filtered ports
PORT    STATE SERVICE  VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     syntax error (connecting)
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     452 syntax error (connecting)
|   SIPOptions:
|     452 syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|     syntax error (connecting)
|_    syntax error (connecting)
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Did not follow redirect to https://transact.playstation.com/
443/tcp open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-server-header: AkamaiNetStorage
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=transact.playstation.com
| Subject Alternative Name: DNS:transact.playstation.com, DNS:www.transact.playstation.com
| Not valid before: 2020-02-26T00:00:00
|_Not valid after:  2022-03-13T23:59:59
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.80%I=7%D=10/16%Time=5F899836%P=x86_64-pc-linux-gnu%r(Hel
SF:lo,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x2
SF:0syntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,3E,"452\x20synt
SF:ax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting
SF:\)\r\n")%r(GetRequest,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n4
SF:52\x20syntax\x20error\x20\(connecting\)\r\n")%r(HTTPOptions,3E,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connec
SF:ting\)\r\n")%r(RTSPRequest,3E,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n452\x20syntax\x20error\x20\(connecting\)\r\n")%r(SSLSessionReq,1F,"
SF:452\x20syntax\x20error\x20\(connecting\)\r\n")%r(TerminalServerCookie,1
SF:F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(TLSSessionReq,1F,"4
SF:52\x20syntax\x20error\x20\(connecting\)\r\n")%r(Kerberos,1F,"452\x20syn
SF:tax\x20error\x20\(connecting\)\r\n")%r(FourOhFourRequest,3E,"452\x20syn
SF:tax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connectin
SF:g\)\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n"
SF:)%r(LDAPSearchReq,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n452\x
SF:20syntax\x20error\x20\(connecting\)\r\n")%r(SIPOptions,155,"452\x20synt
SF:ax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting
SF:\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20erro
SF:r\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\
SF:x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(con
SF:necting\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\
```

pwnXSS result,



Sqlmap result,





Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (jQuery)	GET	https://transact.playstation.com/assets/vendor-9b63638465479f9d366b0648da8bbfbb.js	
	Misconfigured X-Frame-Options Header	GET	https://transact.playstation.com/opensearch.xml	
	Missing X-Frame-Options Header	GET	https://transact.playstation.com/html/weblframeRedirect.html	
	Cookie Not Marked as HttpOnly	GET	http://transact.playstation.com/	
	Expect-CT Not Enabled	GET	https://transact.playstation.com/opensearch.xml	
	Missing X-XSS-Protection Header	GET	https://transact.playstation.com/opensearch.xml	
	Referrer-Policy Not Implemented	GET	https://transact.playstation.com/opensearch.xml	
	SameSite Cookie Not Implemented	GET	http://transact.playstation.com/	
	Email Address Disclosure	GET	https://transact.playstation.com/assets/psst-fe190865ca6ae935c1ae3d1c9c2217e8.js	
	Missing object-src in CSP Declaration	GET	https://transact.playstation.com/opensearch.xml	

Vulnerability title:

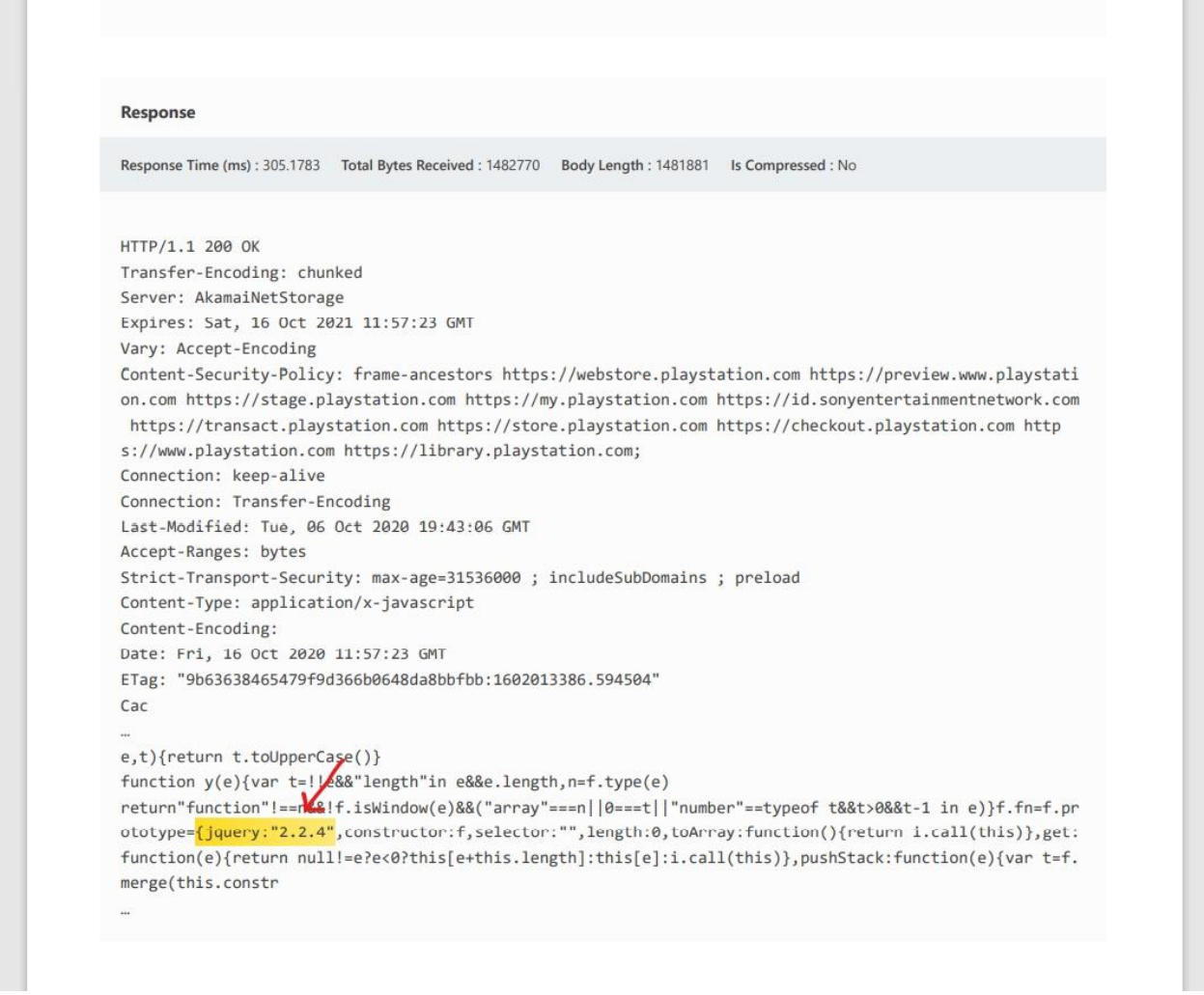
Out-of-date Version (jQuery)

Risk rating:

Severity: Medium

Description:

Netsparker identified the target web site is using jQuery and detected that it is out of date



Response

Response Time (ms) : 305.1783 Total Bytes Received : 1482770 Body Length : 1481881 Is Compressed : No

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: AkamaiNetStorage
Expires: Sat, 16 Oct 2021 11:57:23 GMT
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors https://webstore.playstation.com https://preview.www.playstati
on.com https://stage.playstation.com https://my.playstation.com https://id.sonyentertainmentnetwork.com
 https://transact.playstation.com https://store.playstation.com https://checkout.playstation.com http
s://www.playstation.com https://library.playstation.com;
Connection: keep-alive
Connection: Transfer-Encoding
Last-Modified: Tue, 06 Oct 2020 19:43:06 GMT
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains ; preload
Content-Type: application/x-javascript
Content-Encoding:
Date: Fri, 16 Oct 2020 11:57:23 GMT
ETag: "9b63638465479f9d366b0648da8bbfbb:1602013386.594504"
Cac
…
e,t){return t.toUpperCase()}
function y(e){var t=!!e&&"length"in e&&e.length,n=f.type(e)
return"function"!==n&&!f.isWindow(e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e)}f.fn=f.pr
ototype={jquery:"2.2.4",constructor:f,selector:"",length:0,toArray:function(){return i.call(this)},get:
function(e){return null!=e?e<0?this[e+this.length]:this[e]:i.call(this)},pushStack:function(e){var t=f.
merge(this.constr
…
```

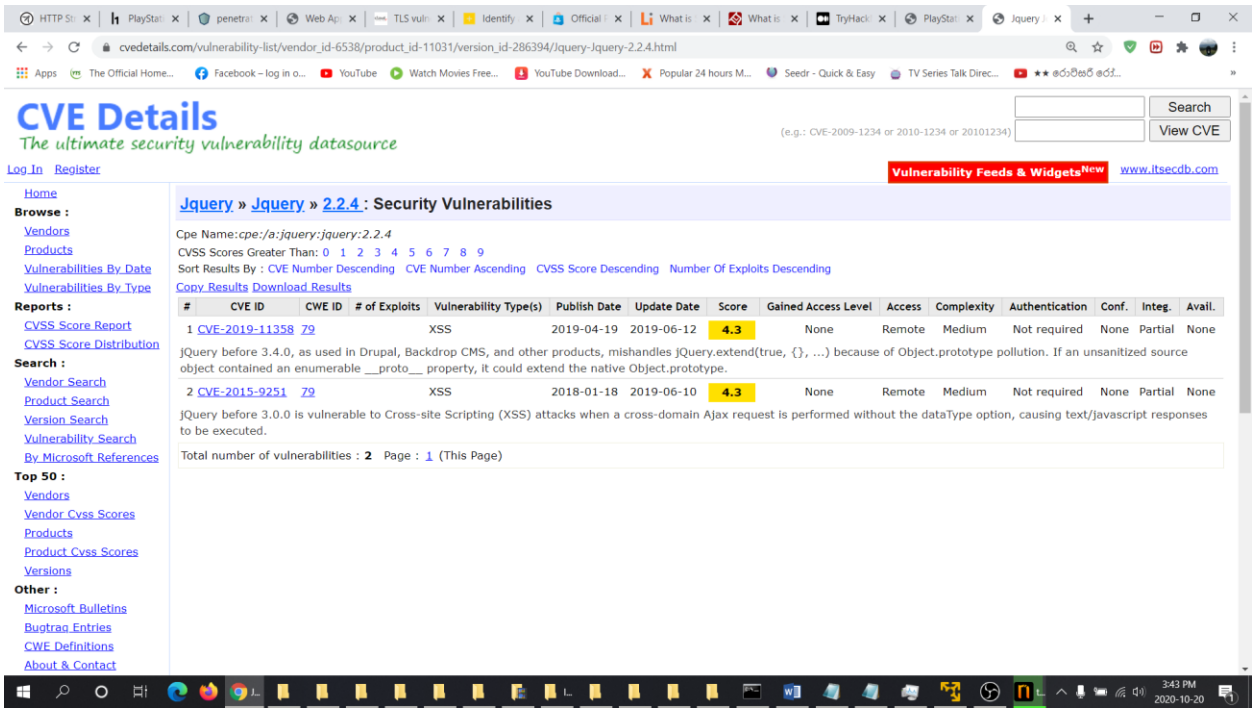
Impact:

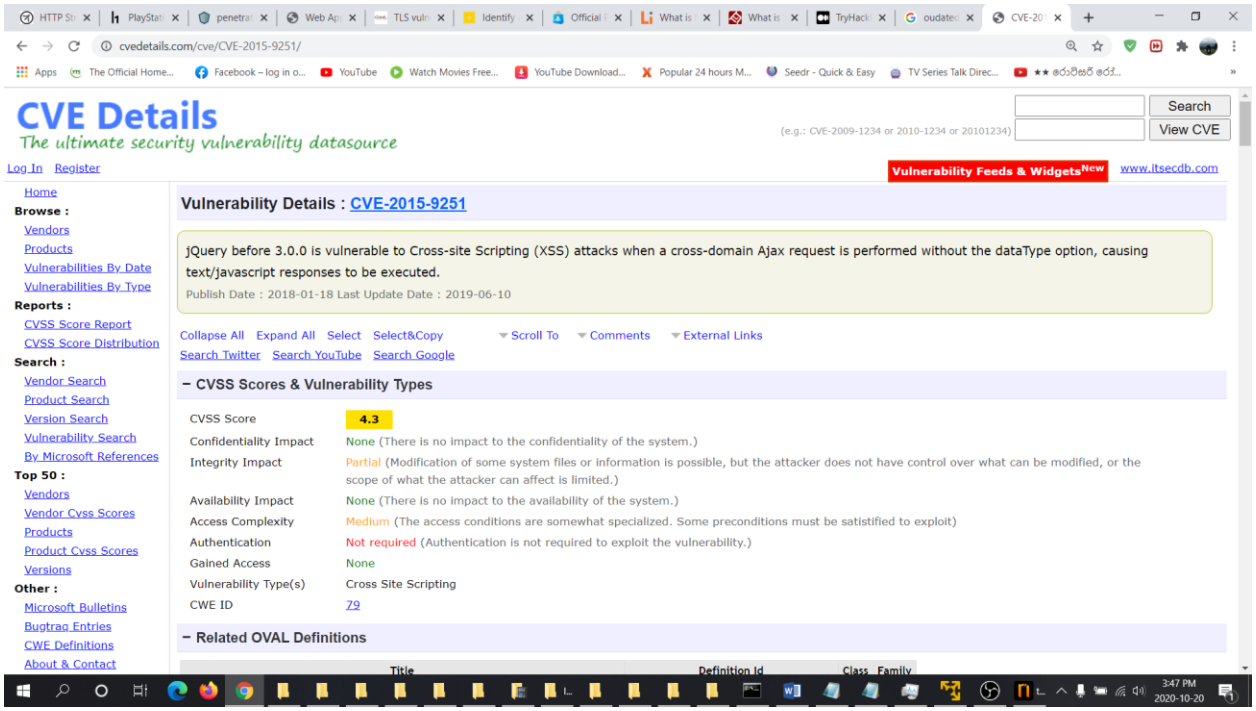
Since this is an old version of the software, it may be vulnerable to attack

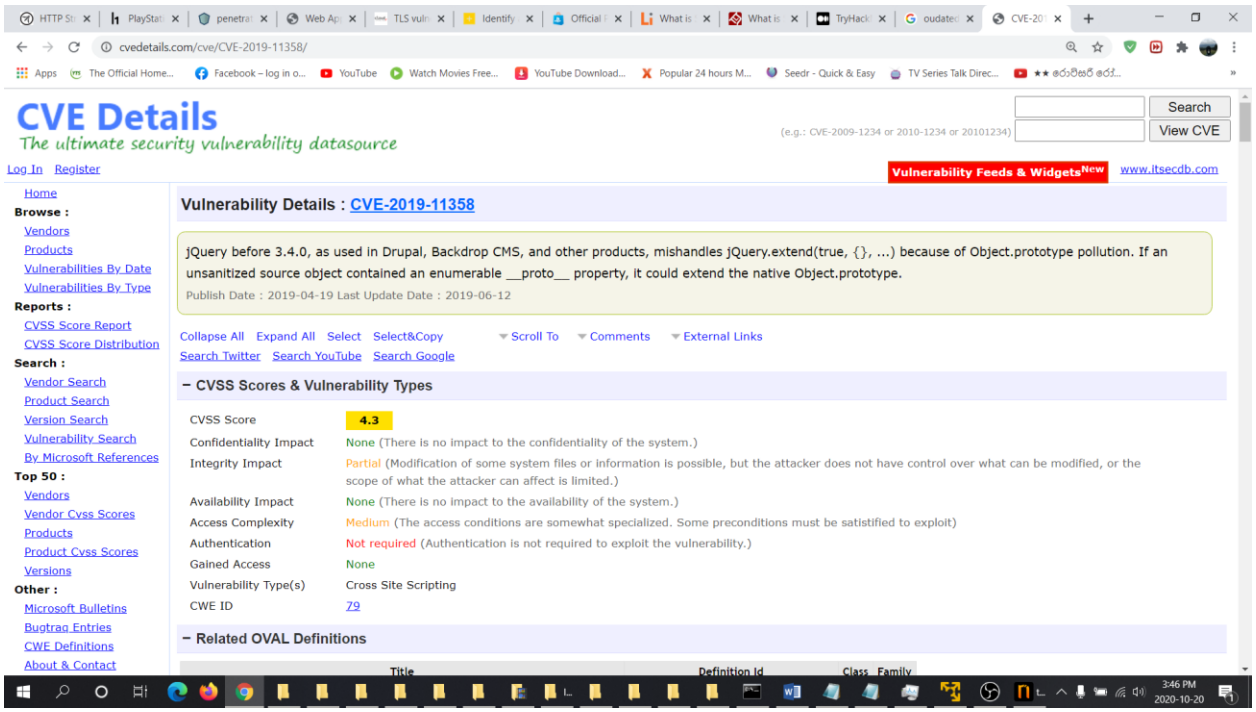
jquery Cross-Site Scripting (XSS) Vulnerability

- jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

These are the vulnerable security attacks for jquery version 2.2.4 according to the https://www.cvedetails.com/vulnerability-list/vendor_id-6538/product_id-11031/version_id-286394/Jquery-Jquery-2.2.4.html




cvedetails.com/cve/CVE-2015-9251/
CVE Details
The ultimate security vulnerability datasource
Search
View CVE
Log In Register
Vulnerability Feeds & Widgets New
www.itsecdb.com
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Vulnerability Details : CVE-2015-9251
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
Publish Date : 2018-01-18 Last Update Date : 2019-06-10
Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google
– CVSS Scores & Vulnerability Types
CVSS Score 4.3
Confidentiality Impact None (There is no impact to the confidentiality of the system.)
Integrity Impact Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact None (There is no impact to the availability of the system.)
Access Complexity Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication Not required (Authentication is not required to exploit the vulnerability.)
Gained Access None
Vulnerability Type(s) Cross Site Scripting
CWE ID 79
– Related OVAL Definitions
Title
Definition Id
Class Family
3:47 PM
2020-10-20


cvedetails.com/cve/CVE-2019-11358/
CVE Details
The ultimate security vulnerability datasource
Search
View CVE
Log In Register
Vulnerability Feeds & Widgets New
www.itsecdb.com
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Vulnerability Details : CVE-2019-11358
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
Publish Date : 2019-04-19 Last Update Date : 2019-06-12
Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google
– CVSS Scores & Vulnerability Types
CVSS Score 4.3
Confidentiality Impact None (There is no impact to the confidentiality of the system.)
Integrity Impact Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact None (There is no impact to the availability of the system.)
Access Complexity Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication Not required (Authentication is not required to exploit the vulnerability.)
Gained Access None
Vulnerability Type(s) Cross Site Scripting
CWE ID 79
– Related OVAL Definitions
Title
Definition Id
Class Family
3:46 PM
2020-10-20

Mitigate threat:

Upgrade your installation of jQuery to the latest stable version.

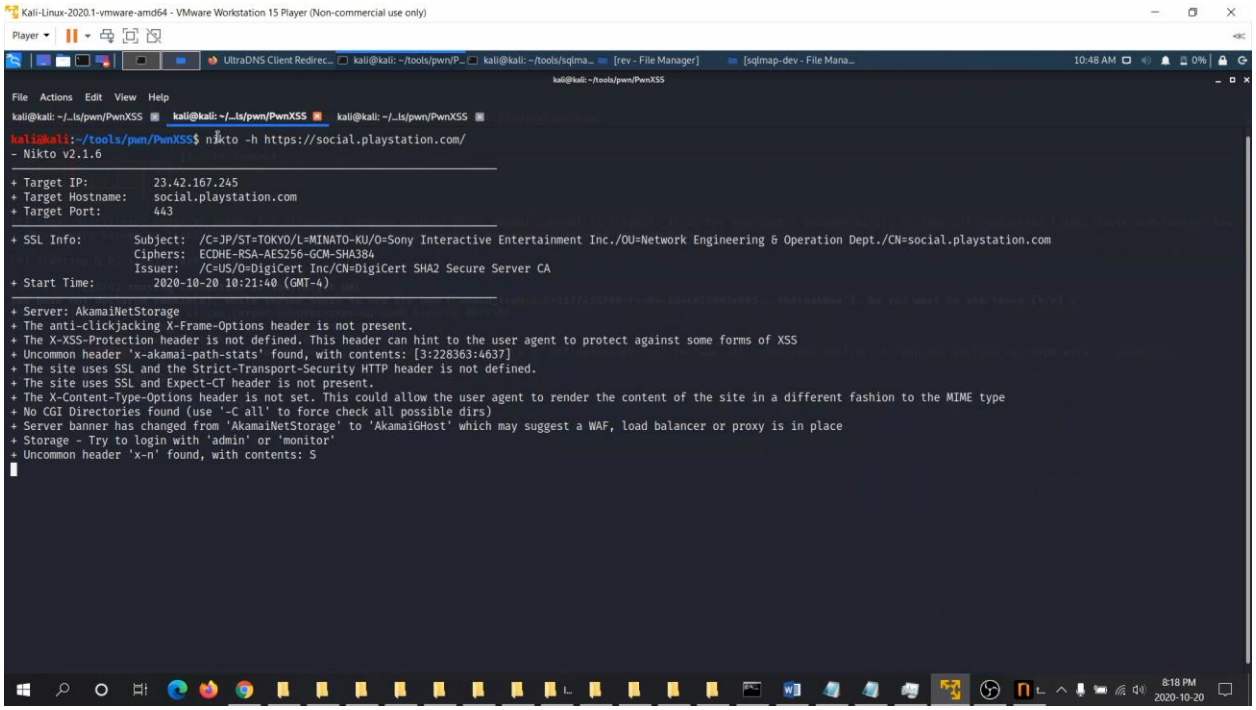
These are the missing headers that should include,

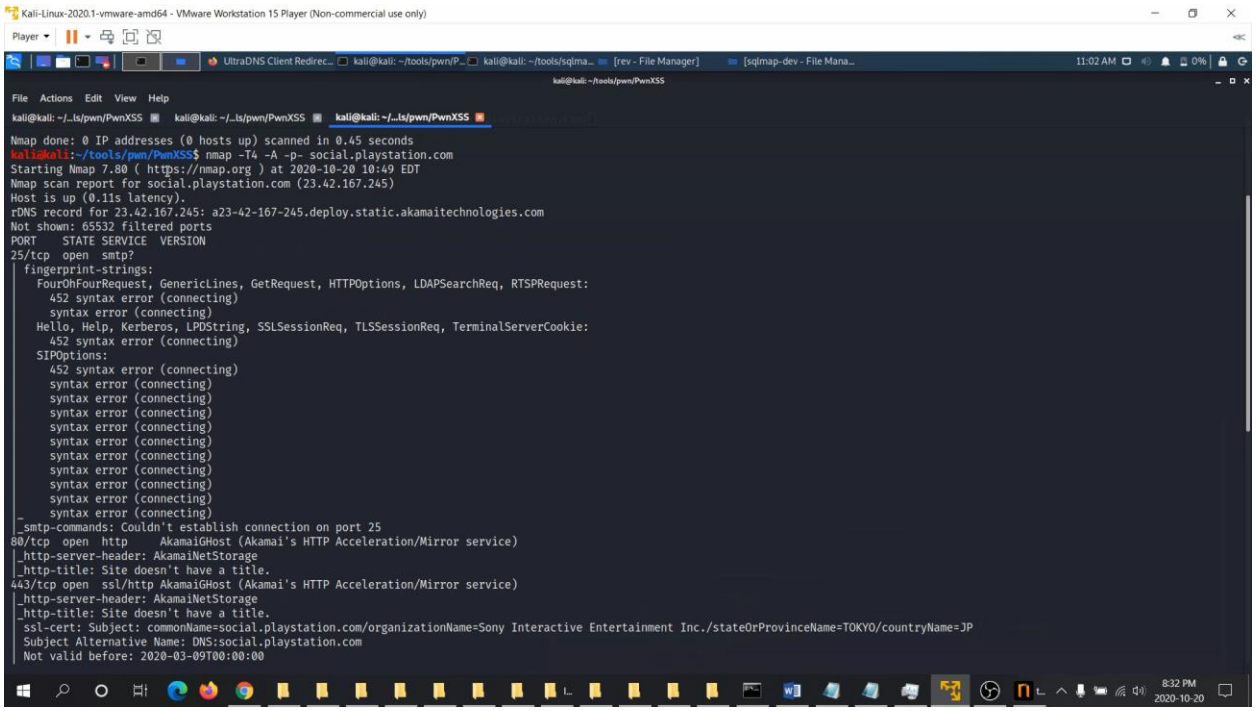
Missing Headers

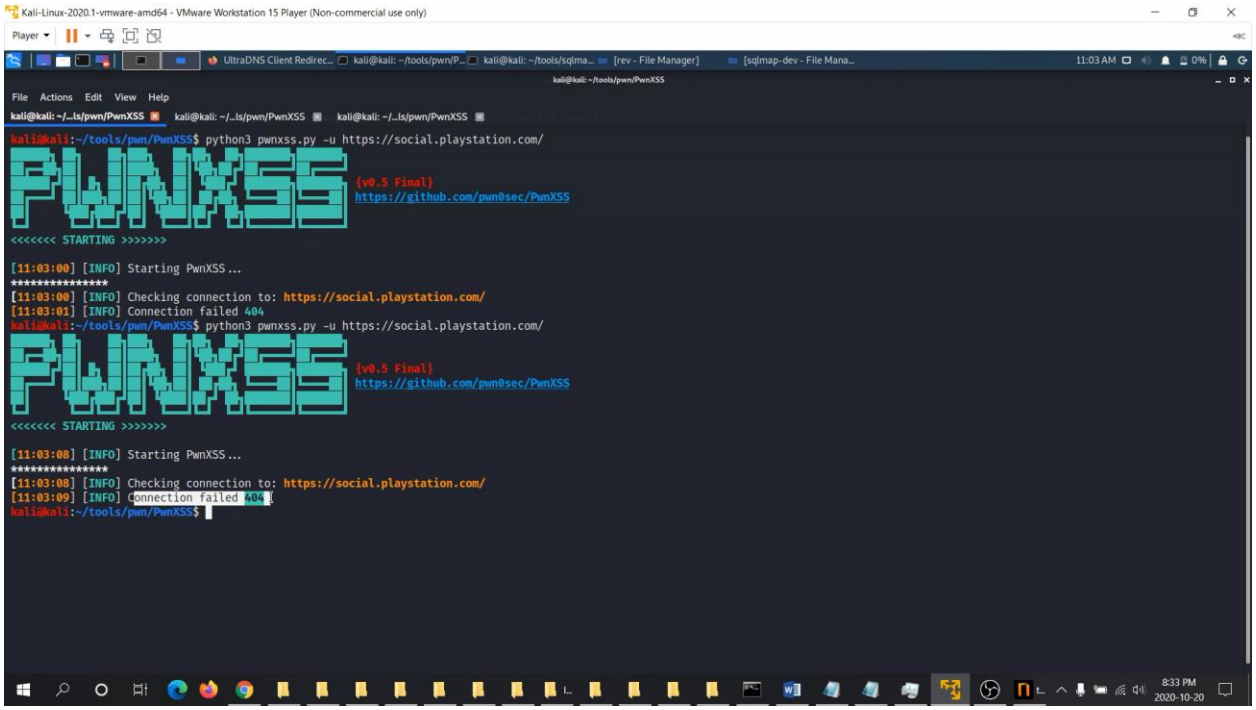
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

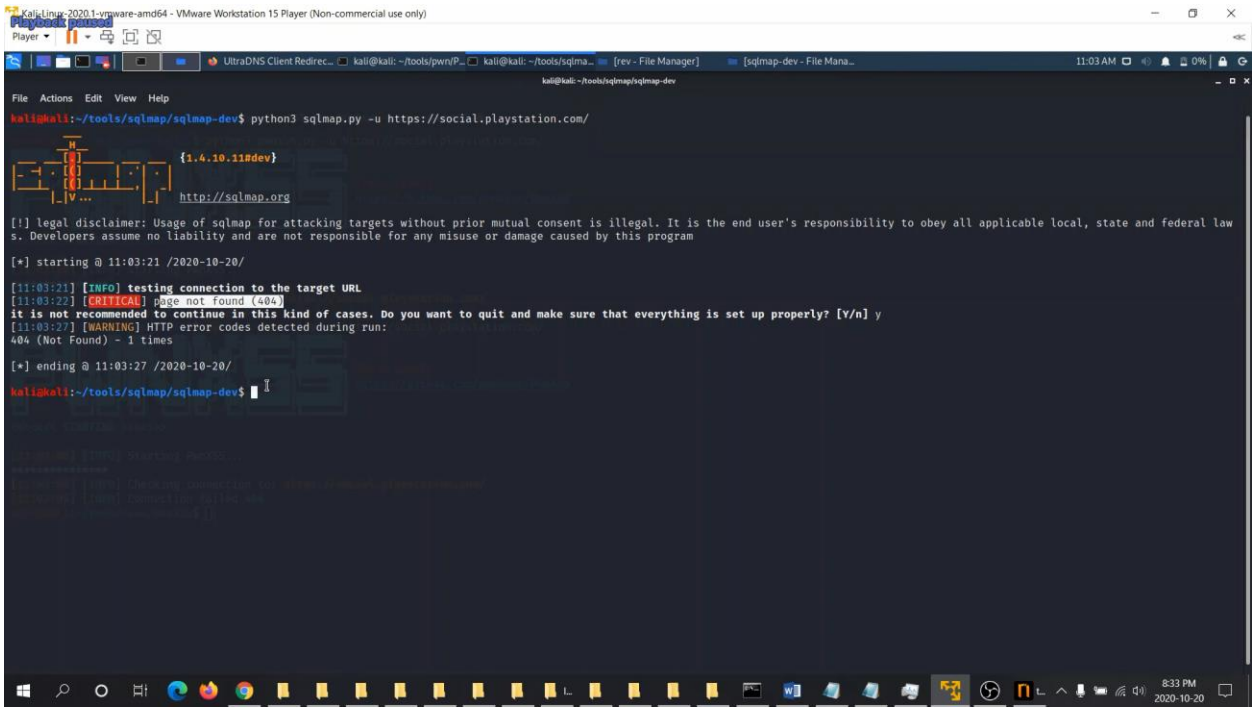
5.https://social.playstation.com/

Here are the results using recon tools,

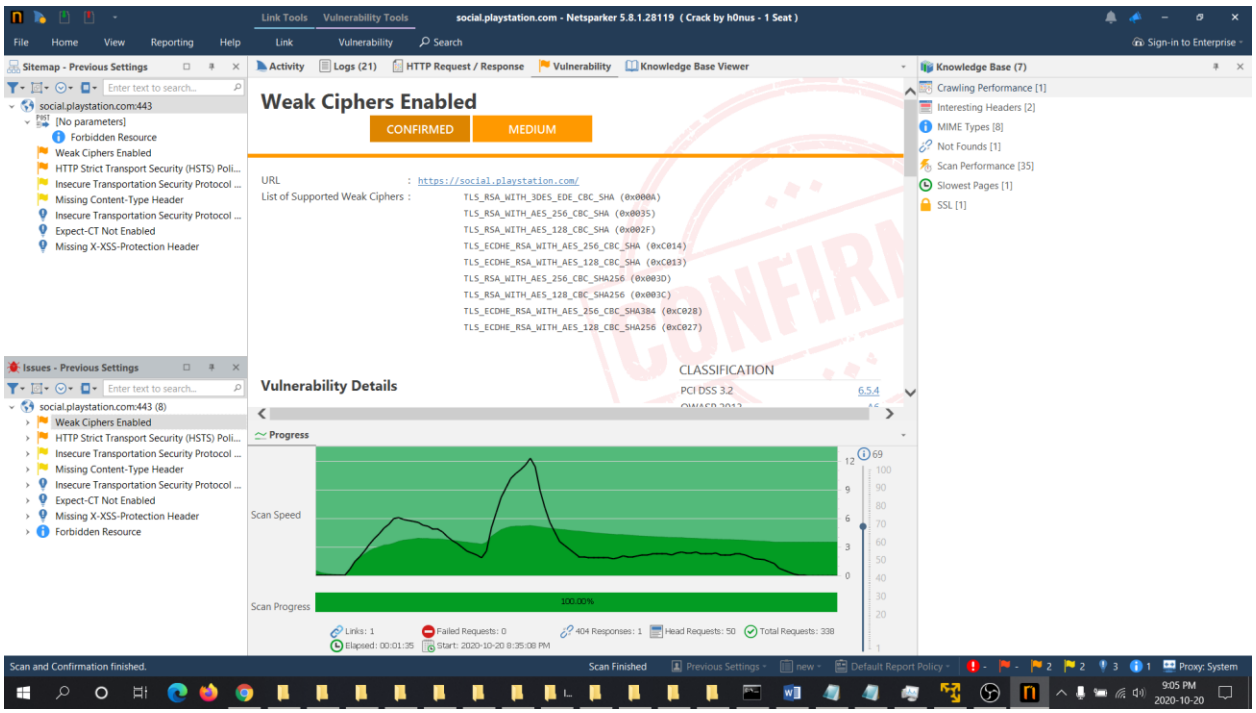



Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
kali@kali: ~/tools/pwn/PwnXSS
File Actions Edit View Help
kali@kali: ~/...ls/pwn/PwnXSS
kali@kali: ~/...ls/pwn/PwnXSS
kali@kali: ~/...ls/pwn/PwnXSS
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.45 seconds
kali@kali:~/tools/pwn/PwnXSS$ nmap -T4 -A -p- social.playstation.com
Starting Nmap 7.80 (https://nmap.org) at 2020-10-20 10:49 EDT
Nmap scan report for social.playstation.com (23.42.167.245)
Host is up (0.11s latency).
rDNS record for 23.42.167.245: a23-42-167-245.deploy.static.akamaitechnologies.com
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp?
| fingerprint-strings:
| FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
| 452 syntax error (connecting)
| syntax error (connecting)
| Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
| 452 syntax error (connecting)
| SIPOptions:
| 452 syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
| syntax error (connecting)
|_
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-server-header: AkamaiNetStorage
|_http-title: Site doesn't have a title.
443/tcp open ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-server-header: AkamaiNetStorage
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=social.playstation.com/organizationName=Sony Interactive Entertainment Inc./stateOrProvinceName=TOKYO/countryName=JP
| Subject Alternative Name: DNS:social.playstation.com
| Not valid before: 2020-03-09T00:00:00
8:32 PM
2020-10-20


Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
kali@kali: ~/tools/pwn/PwnXSS
File Actions Edit View Help
kali@kali: ~/...ls/pwn/PwnXSS
kali@kali: ~/...ls/pwn/PwnXSS
kali@kali: ~/...ls/pwn/PwnXSS
kali@kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://social.playstation.com/
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<<< STARTING >>>>>>>
[11:03:00] [INFO] Starting PwnXSS...
****
[11:03:00] [INFO] Checking connection to: https://social.playstation.com/
[11:03:01] [INFO] Connection failed 404
kali@kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://social.playstation.com/
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<<< STARTING >>>>>>>
[11:03:08] [INFO] Starting PwnXSS...
****
[11:03:08] [INFO] Checking connection to: https://social.playstation.com/
[11:03:09] [INFO] Connection failed 404
kali@kali:~/tools/pwn/PwnXSS$
8:33 PM
2020-10-20



After the scan using netsparker I got the same issues like in the previous domains and I have already explained about them.



These are the missing headers that should include,

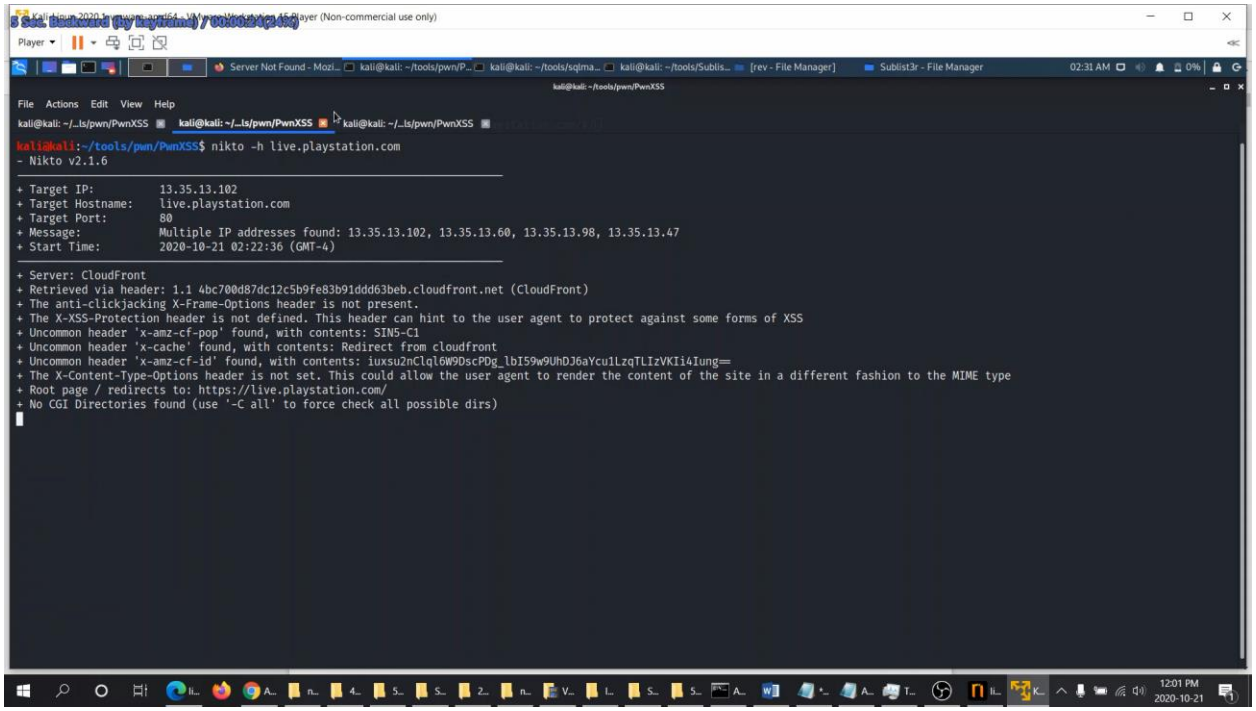
Missing Headers

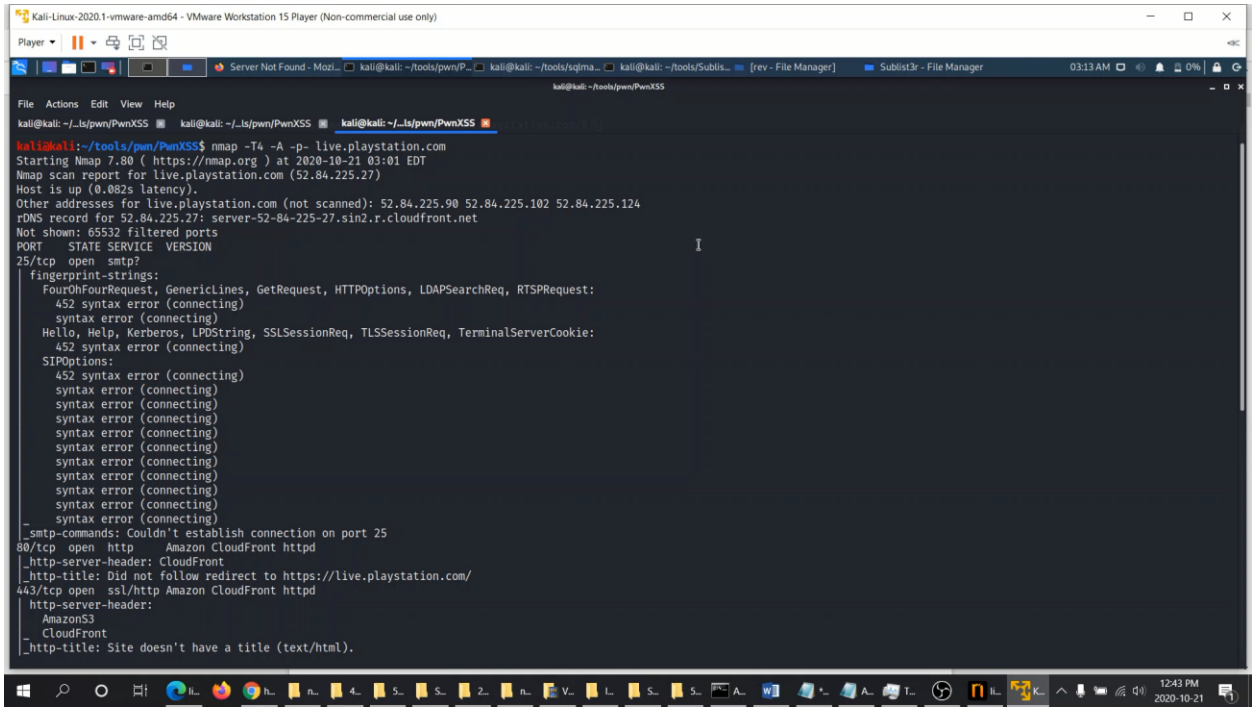
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

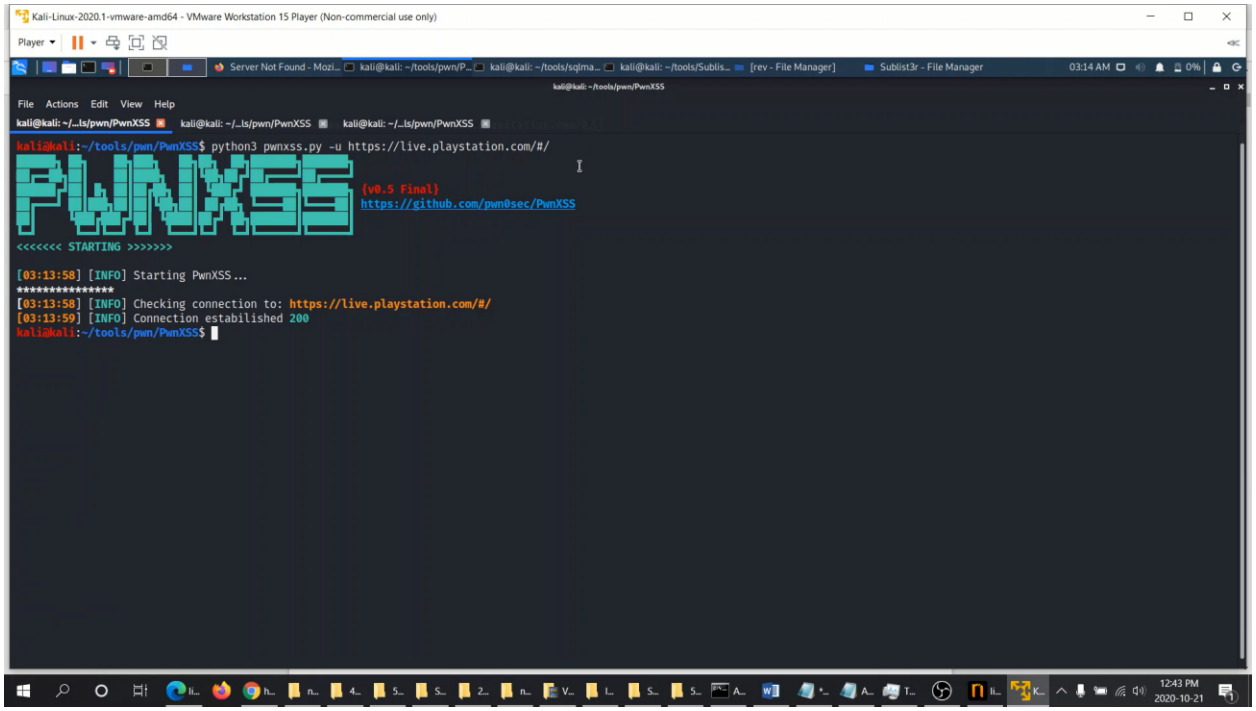
6. https://live.playstation.com/#/

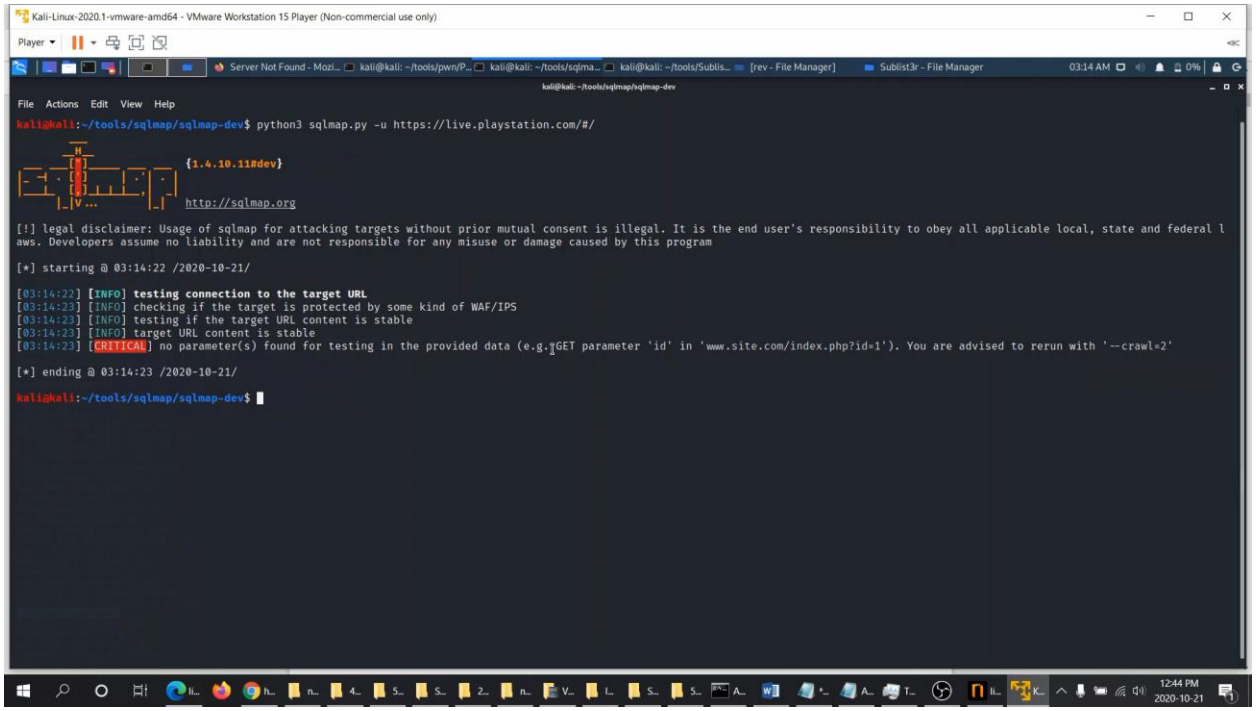
Here are the results using recon tools,

After the scan using linux tools we cannot see any important issues here.




Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali:~/tools/pwn/PwnXSS$ nmap -T4 -A -p- live.playstation.com
Starting Nmap 7.80 (https://nmap.org) at 2020-10-21 03:01 EDT
Nmap scan report for live.playstation.com (52.84.225.27)
Host is up (0.082s latency).
Other addresses for live.playstation.com (not scanned): 52.84.225.90 52.84.225.102 52.84.225.124
rDNS record for 52.84.225.27: server-52-84-225-27.sin2.r.cloudfront.net
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp?
| fingerprint-strings:
FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
452 syntax error (connecting)
syntax error (connecting)
Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
452 syntax error (connecting)
SIPOptions:
452 syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
syntax error (connecting)
_smtp-commands: Couldn't establish connection on port 25
80/tcp open http Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://live.playstation.com/
443/tcp open ssl/http Amazon CloudFront httpd
| http-server-header:
AmazonS3
CloudFront
|_http-title: Site doesn't have a title (text/html).

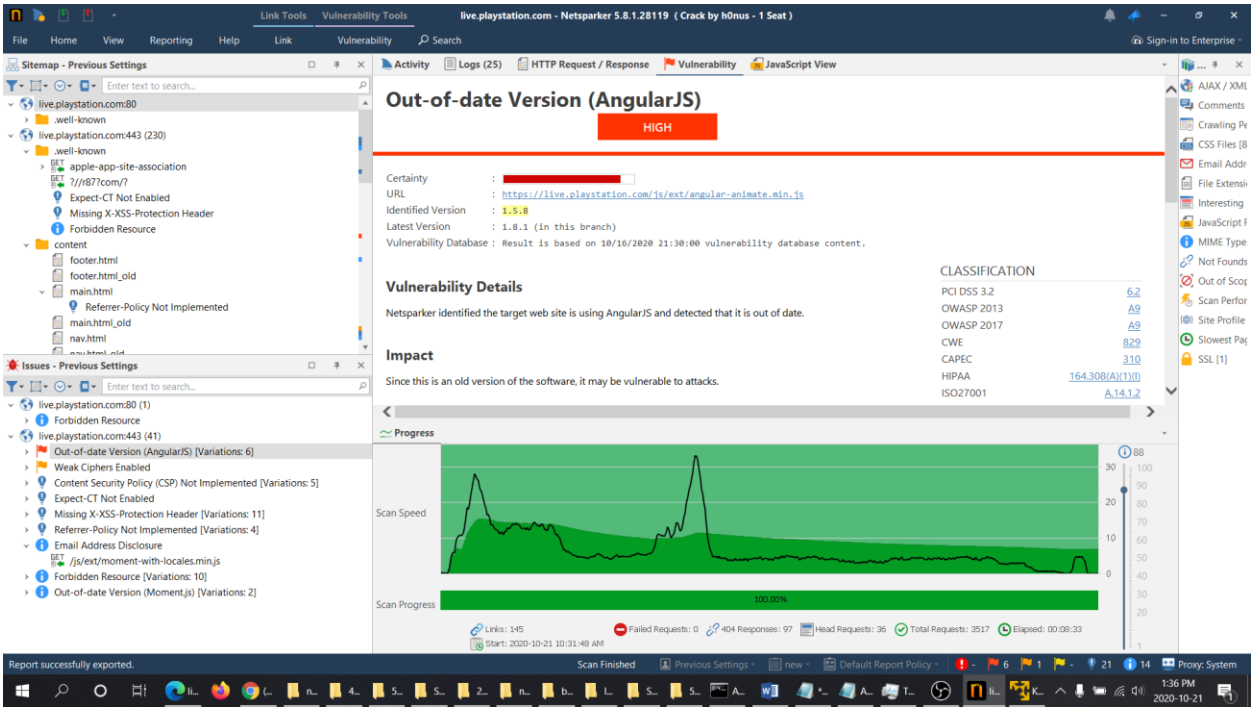

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://live.playstation.com/#/
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<<< STARTING >>>>>>>
[03:13:58] [INFO] Starting PwnXSS...
****
[03:13:58] [INFO] Checking connection to: https://live.playstation.com/#/
[03:13:59] [INFO] Connection estabilished 200
kali@kali:~/tools/pwn/PwnXSS$



But netsparker able to capture some important issues after the scan.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (AngularJS)	GET	https://live.playstation.com/js/ext/angular-sanitize.min.js	
	Weak Ciphers Enabled	GET	https://live.playstation.com/	
	Content Security Policy (CSP) Not Implemented	GET	https://live.playstation.com/	
	Expect-CT Not Enabled	GET	https://live.playstation.com/.well-known/	
	Missing X-XSS-Protection Header	GET	https://live.playstation.com/.well-known/	
	Referrer-Policy Not Implemented	GET	https://live.playstation.com/content/main.html	
	Email Address Disclosure	GET	https://live.playstation.com/js/ext/moment-with-locales.min.js	
	Out-of-date Version (Moment.js)	GET	https://live.playstation.com/	
	Forbidden Resource	GET	https://live.playstation.com/.well-known/	



Vulnerability title:

Out-of-date Version (AngularJS)

Risk rating:

Severity: High

Description:

Netsparker identified the target web site is using AngularJS and detected that it is out of date.This currently running in version 1.5.8.

Response

Response Time (ms) : 349.8615 Total Bytes Received : 6438 Body Length : 5861 Is Compressed : No

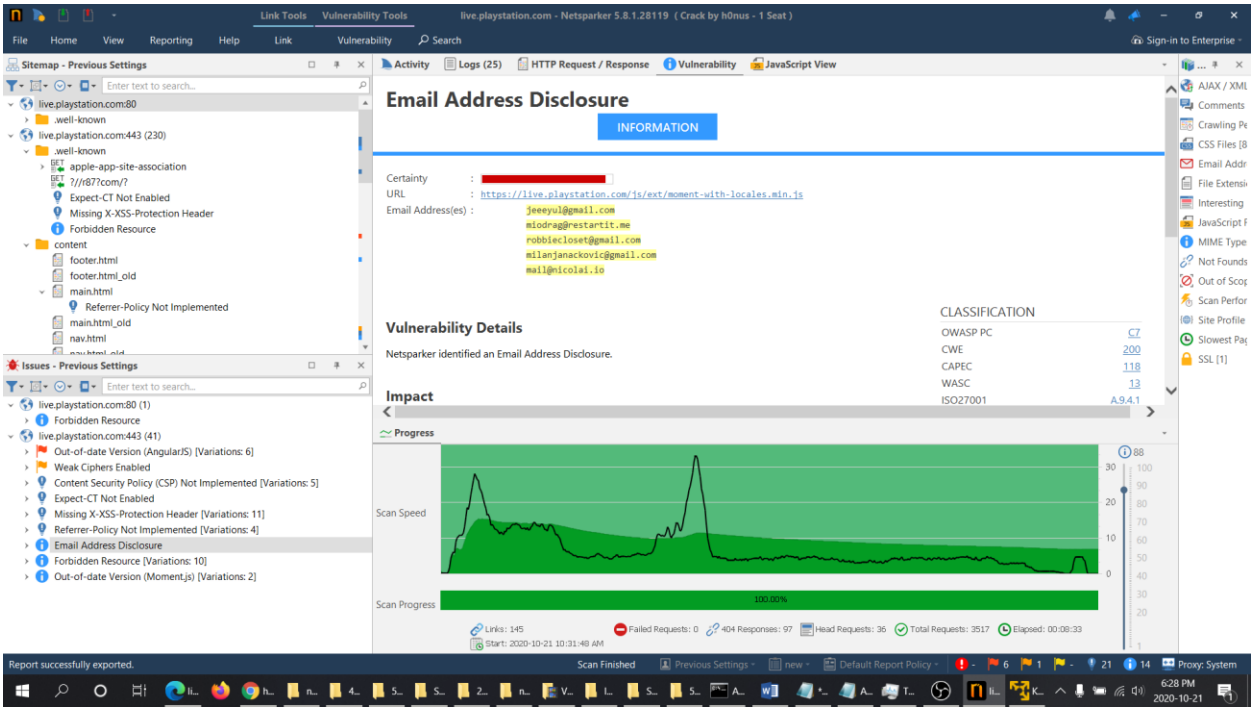
```
HTTP/1.1 200 OK
Server: AmazonS3
X-Cache: Hit from cloudfront
Connection: keep-alive
Via: 1.1 b95596d6887b20449c59c2fc9d141c4a.cloudfront.net (CloudFront)
Content-Length: 5861
Last-Modified: Fri, 31 Aug 2018 20:13:29 GMT
Accept-Ranges: bytes
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
Content-Type: application/javascript
X-Amz-Cf-Pop: SIN5-C1
X-Amz-Cf-Id: BSf3SrKkR380syr6DZ-l9PsbJ6l7T0fxTeoR4FHCLBDf8YnJu2c_UQ==
Age: 28198
Date: Tue, 20 Oct 2020 21:12:03 GMT
ETag: "1ed87cdd5af63f804f
…
/javascript
X-Amz-Cf-Pop: SIN5-C1
X-Amz-Cf-Id: BSf3SrKkR380syr6DZ-l9PsbJ6l7T0fxTeoR4FHCLBDf8YnJu2c_UQ==
Age: 28198
Date: Tue, 20 Oct 2020 21:12:03 GMT
ETag: "1ed87cdd5af63f804fb0889392dd3917"

/*
AngularJS v1.5.8
(c) 2010-2016 Google, Inc. http://angularjs.org
License: MIT
*/
(function(s,g){'use strict';function H(g){var l=[];t(l,A).chars(g);return l.join("")}var B=g.$$minErr
("$sanitize"),C,l,D,E,q,A,F,t;g.
```

Impact:

Since this is an old version of the software, it may be vulnerable to attacks like XSS.

Mitigate threat:

The AngularJS should upgrade to the latest stable version.



Vulnerability title:

Email Address Disclosure

Risk rating:

Severity: Information

Description:

Netsparker identified an Email Address Disclosure

```
//! author : Jeeeyul Lee <jeeeyul@gmail.com>
a.defineLocale("ko",{months:"1월_2월_3월_4월_5월_6월_7월_8월_9월_10월_11월_12월".split("_"),monthsShor
t:"1월_2월_3월_4월_5월_6월_7월_8월_9월_10월_11월_12월".split("_"),weekdays:"일요일_월요일_화요일_수요일_목요
일_금요일_토요일".split("_"),week
…
d,d:Zd,dd:Yd,M:Zd,MM:Yd,y:Zd,yy:Yd},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:
4}});
//! moment.js locale configuration
//! locale : Montenegrin [me]
//! author : Miodrag Nikač <miodrag@restartit.me> : https://github.com/miodragnikac
var ph={words:{m:["jedan minut","jednog minuta"],mm:["minut","minuta","minuta"],h:["jedan sat","jednog
 sata"],hh:["sat","sata","sati"],dd:["dan","dana","dana"],MM:[
…
:ph.translate,y:"godinu",yy:ph.translate},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,
doy:7}}),
//! moment.js locale configuration
//! locale : Maori [mi]
//! author : John Corrigan <robbiecloset@gmail.com> : https://github.com/johnideal
a.defineLocale("mi",{months:"Kohi-tāte_Hui-tanguru_Poutū-te-rangi_Paenga-whāwhā_Haratua_Pipiri_Hōngoing
oi_Here-turi-kōkā_Mahuru_Whiringa-ā-nuku_Whiringa-ā-rangi_Hakihe
…
"një vit",yy:"%d vite"},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:4}});
//! moment.js locale configuration
//! locale : Serbian Cyrillic [sr-cyrl]
//! author : Milan Janačković<milanjanackovic@gmail.com> : https://github.com/milan-j
var Nh={words:{m:["један минут","једне минуте"],mm:["минут","минуте","минута"],h:["један сат","једног с
```



```
ата"],hh:["сат","сата","сати"],dd:["дан","дана","дана"],MM:["месец
…
translate,y:"годину",yy:Nh.translate},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:
7}});
//! moment.js locale configuration
//! locale : Serbian [sr]
//! author : Milan Janačković<milanjanackovic@gmail.com> : https://github.com/milan-j
```

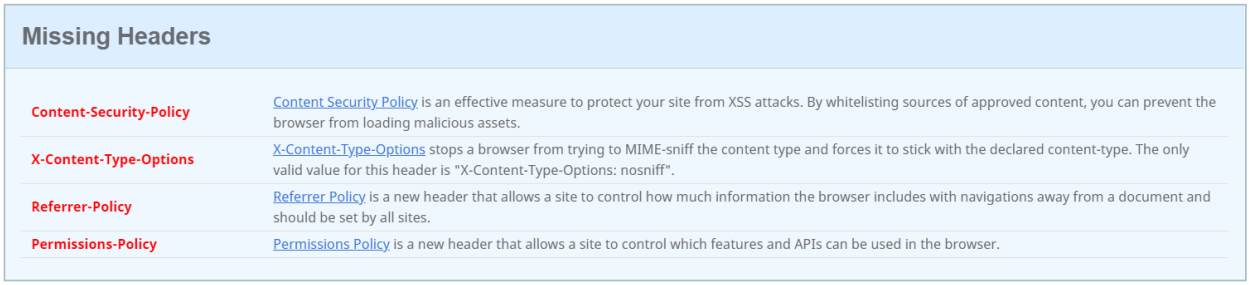
Impact:

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Mitigate threat:

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

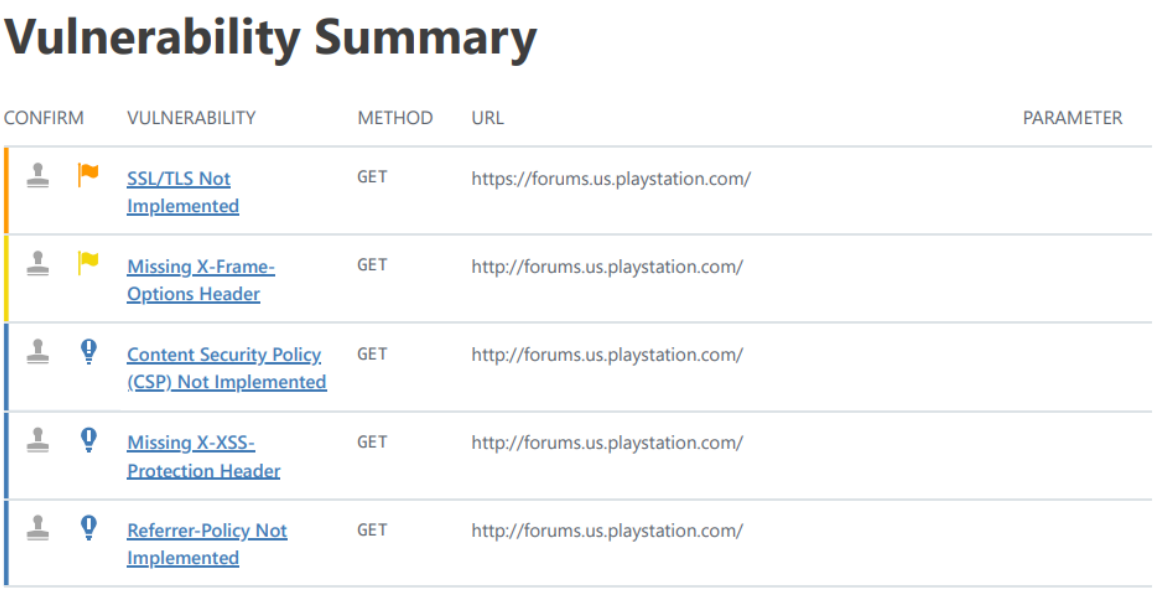
These are the missing headers that should include,



Missing Headers

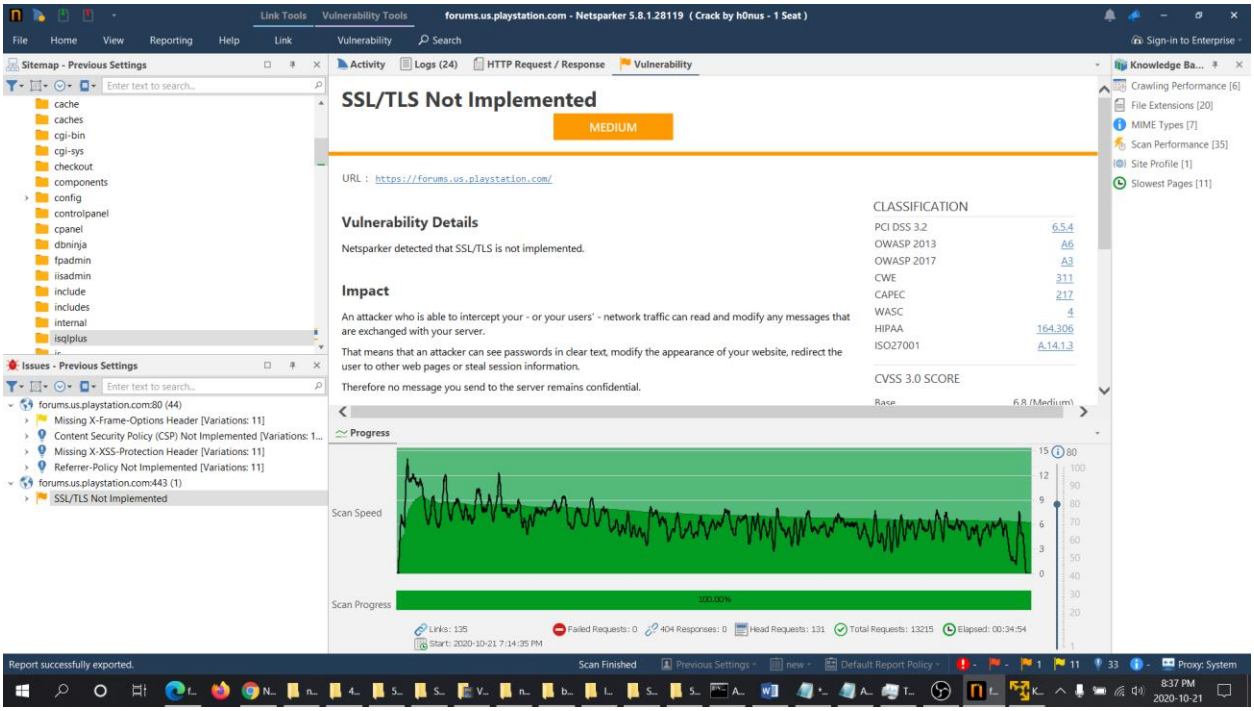
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

7. https://forums.us.playstation.com/



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	SSL/TLS Not Implemented	GET	https://forums.us.playstation.com/	
	Missing X-Frame-Options Header	GET	http://forums.us.playstation.com/	
	Content Security Policy (CSP) Not Implemented	GET	http://forums.us.playstation.com/	
	Missing X-XSS-Protection Header	GET	http://forums.us.playstation.com/	
	Referrer-Policy Not Implemented	GET	http://forums.us.playstation.com/	



Vulnerability title:

SSL/TLS Not implemented

Risk rating:

Severity: Information

Description:

Netsparker detected that SSL/TLS is not implemented.

Impact:

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

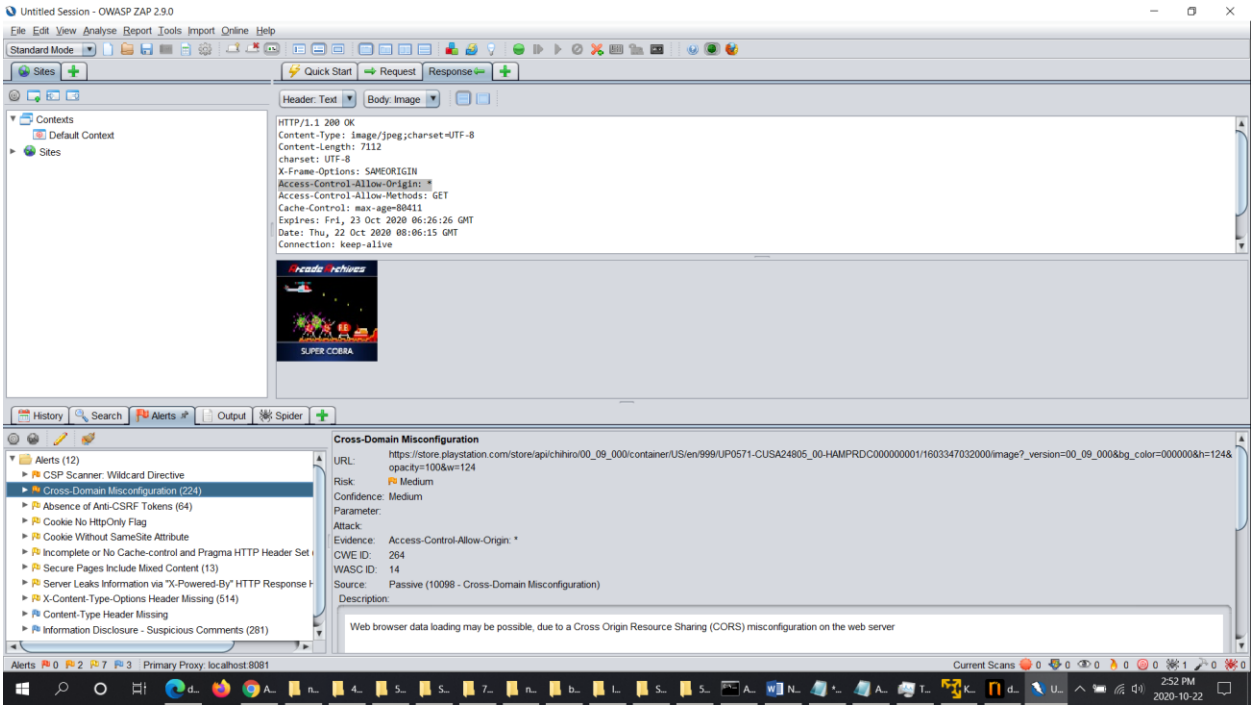
Therefore no message you send to the server remains confidential.

Mitigate threat:

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

8.store.playstation.com

This domain scanned with OWASP ZAP tool and identified some important issues.



Vulnerability title:

Cross domain misconfiguration

Risk rating:

Severity:Medium

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server. The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat

Impact:

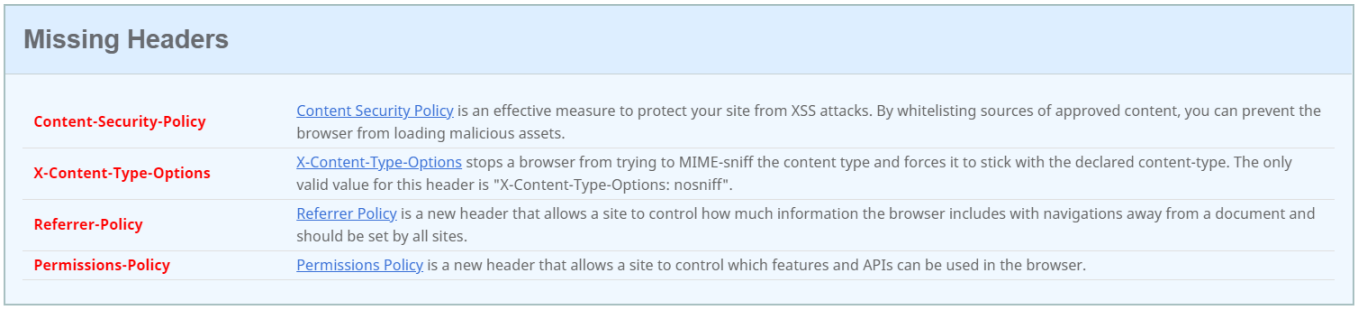
This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Mitigate threat:

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

These are the missing headers that should include,



Reference

- TLS certificate issue-
  - https://www.cloudinsidr.com/content/known-attack-vectors-_against-tls-implementation-vulnerabilities/
  - https://www.helpnetsecurity.com/2014/02/25/identify-and-fix-vulnerabilities-in-your-ssl-certificates/

- Strict transport security not enforced –
  - https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

- Security headers-
  - https://securityheaders.com/